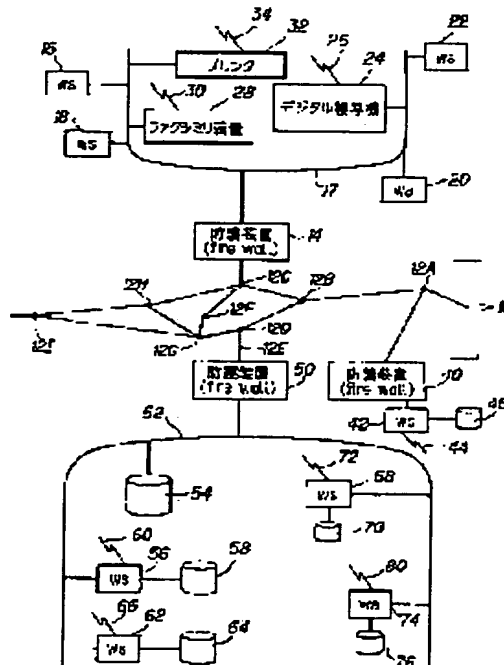


(11)Publication number : 10-145610
(43)Date of publication of application : 29.05.1998

(30)Priority
Priority number : 96 733134 Priority date : 16.10.1996 Priority country : US

SOLUTION: Office equipments 24, 28, 32 recognizing only approved information monitor each status of the office equipments 24, 28, 32 through the Internet 10 and/or a content of a message is monitored by a security center to send the message to a controlled data center. A log of the message sent to the Internet 10 is reserved through protection devices 14, 40, 50 and only the message received and checked by the security center is sent through the Internet 10 via the protection devices 14, 40, 50, then the message is compared with the message received by the security center.



[Date of request for examination]	14.05.2002
[Date of sending the examiner's decision of rejection]	
[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]	
[Date of final disposal for application]	
[Patent number]	

[Date of registration]

[Number of appeal against examiner's decision
of rejection]

[Date of requesting appeal against examiner's
decision of rejection]

[Date of extinction of right]

Copyright (C); 1998,2003 Japan Patent Office

(19)日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11)特許出願公開番号

特開平10-145610

(43)公開日 平成10年(1998)5月29日

(51)Int.Cl.⁶
 H 0 4 N 1/44
 B 4 1 J 29/00
 29/38
 G 0 3 G 21/00 3 9 6
 H 0 4 N 1/00 1 0 7

識別記号

F I

H 0 4 N 1/44
 B 4 1 J 29/38 Z
 G 0 3 G 21/00 3 9 6
 H 0 4 N 1/00 1 0 7 Z
 B 4 1 J 29/00 U

審査請求 未請求 請求項の数58 O L (全 31 頁)

(21)出願番号 特願平9-284109

(22)出願日 平成9年(1997)10月16日

(31)優先権主張番号 08/733 134

(32)優先日 1996年10月16日

(33)優先権主張国 米国 (U S)

(71)出願人 000006747

株式会社リコー

東京都大田区中馬込1丁目3番6号

(72)発明者 テツロウ モトヤマ

アメリカ合衆国, カリフォルニア州

95134-8800, サン ホセ, オーチャード

パークウェイ ドライブ 3001, リコー

コーポレーション エス・ピー・ビー内

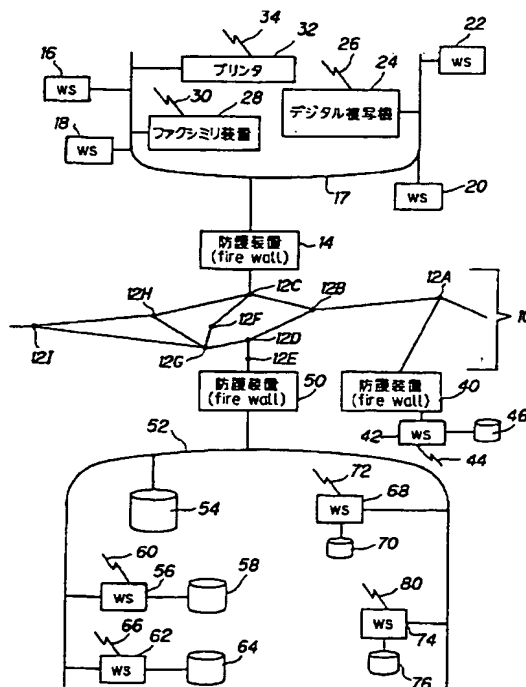
(74)代理人 弁理士 酒井 宏明

(54)【発明の名称】 通信処理方法および通信処理システム

(57)【要約】

【課題】 発信無接続通信が確実に承認され、かつその秘密が保持されるようにすること。

【解決手段】 承認された情報だけが認められたビジネスオフィス機器24、28、32からインターネット10を通じてそのビジネスオフィス機器24、28、32のステータスをモニターし、そして/または制御するデータ・センターに送られるようにするため、そのメッセージの内容がセキュリティ・センターによってモニターされる。防護装置14、40、50を通じてインターネット10に送られるメッセージのログは保存され、セキュリティ・センターにより受信されチェックされたメッセージだけが防護装置14、40、50を介し、インターネット10を通じて送られるようにするために、セキュリティ・センターによって受信されたメッセージと比較される。



【特許請求の範囲】

【請求項1】 電気機械式センサを有する機械からデータ・センターへの通信を処理する通信処理方法において、

前記データ・センターに送られる情報を含んだメッセージを作成する作成工程と、

前記メッセージを前記機械から防護装置に送信する送信工程と、

前記メッセージをセキュリティ装置に送信する送信工程と、

前記セキュリティ装置によって前記メッセージを分析する分析工程と、

を含んでいることを特徴とする通信処理方法。

【請求項2】 さらに、前記メッセージを前記セキュリティ装置に送信する送信工程が、前記メッセージを前記防護装置によって受信されたメッセージを前記セキュリティ装置に送信する送信工程を含んでいることを特徴とする請求項1に記載の通信処理方法。

【請求項3】 さらに、前記分析工程で前記メッセージが認められたメッセージでないと判定された場合にセキュリティ動作を実行するセキュリティ工程を含んでいることを特徴とする請求項1に記載の通信処理方法。

【請求項4】 さらに、セキュリティ動作を実行するセキュリティ工程が、前記防護装置を通過して来るメッセージを禁止する禁止工程を含んでいることを特徴とする請求項1に記載の通信処理方法。

【請求項5】 さらに、セキュリティ動作を実行するセキュリティ工程が、前記防護装置を通過して来る、さらなるメッセージを禁止する禁止工程を含んでいることを特徴とする請求項1に記載の通信処理方法。

【請求項6】 さらに、前記防護装置に送られるメッセージを、前記防護装置に送られる前に暗号化する暗号化工程と、

前記防護装置から受信された暗号化されたメッセージをセキュリティ装置により解読する解読工程と、

を含んでいることを特徴とする通信処理方法。

【請求項7】 さらに、前記防護装置を通じて発信されるメッセージをログ内にロギングするロギング工程を含んでおり、前記分析工程が、前記セキュリティ装置で受信されるメッセージを前記防護装置を通じて発信されるメッセージのログと比較する比較工程を含んでいることを特徴とする請求項1に記載の通信処理方法。

【請求項8】 さらに、前記セキュリティ装置で受信されたメッセージと比較する比較工程で、前記防護装置を通じて発信されるメッセージの一つが、セキュリティ装置によって受信された対応するメッセージと合致していない場合に、前記セキュリティ装置で受信されたメッセージの一つが前記防護装置を通じて発信されるメッセージの対応するものと合致しないことを示す警告を出力する警告工程を含んでいることを特徴とする請求項

7に記載の通信処理方法。

【請求項9】 前記メッセージをセキュリティ装置に送信する送信工程で、前記防護装置の一部であるセキュリティ装置にそのメッセージを送信する送信工程を含んでいることを特徴とする請求項1に記載の通信処理方法。

【請求項10】 メッセージを作成する作成工程が、前記機械の電気機械式センサから受信された情報を含むメッセージを作成する作成工程を含んでいることを特徴とする請求項1に記載の通信処理方法。

【請求項11】 メッセージを作成する作成工程が、ビジネスオフィス機器である前記機械の電気機械式センサから受信された情報を含むメッセージを作成する作成工程を含んでいることを特徴とする請求項10に記載の通信処理方法。

【請求項12】 前記メッセージを前記セキュリティ装置に送信する送信工程が、

前記メッセージを前記防護装置から前記セキュリティ装置に送信する送信工程と、前記メッセージを前記機械から前記セキュリティ装置に送信する送信工程と、を含んでおり、

前記分析工程が、

前記セキュリティ装置によって、前記セキュリティ装置が前記機械から受信した前記メッセージを、前記防護装置から前記セキュリティ装置が受信したメッセージと比較する比較工程を含んでいることを特徴とする請求項1に記載の通信処理方法。

【請求項13】 さらに、前記メッセージを前記防護装置に送信する前に、その防護装置に送信されるメッセージを暗号化する暗号化工程と、

前記防護装置からのメッセージを前記セキュリティ装置に送信する送信工程がそのメッセージを暗号化する暗号化工程と、

さらに、前記セキュリティ装置によって、前記防護装置から受信された暗号化されたメッセージを解読する解読工程と、

前記機械から受信された前記メッセージを解読されたメッセージと比較する比較工程と、

を含んでいることを特徴とする請求項12に記載の通信処理方法。

【請求項14】 前記メッセージを前記機械から前記セキュリティ装置に送信する送信工程が、前記メッセージを非暗号化形式で送信する送信工程を含んでいることを特徴とする請求項13に記載の通信処理方法。

【請求項15】 さらに、前記防護装置から発信されるメッセージをロギングするロギング工程と、

前記セキュリティ装置で受信されたメッセージを前記防護装置を介して送信され、ログされたメッセージと比較する比較工程と、

を含んでいることを特徴とする請求項12に記載の通信処理方法。

【請求項16】 さらに、前記セキュリティ装置で受信されたメッセージを比較する比較工程で、前記防護装置を介して送られるメッセージの一つが前記セキュリティ装置によって受信されたメッセージと合致しないと判断された場合に、前記セキュリティ装置に送信されたメッセージの一つが前記防護装置を通じて発信されるメッセージの対応するものと合致しないことを示す警告を出す警告工程を含んでいることを特徴とする請求項15に記載の通信処理方法。

【請求項17】 メッセージを作成する前記作成工程が前記機械の電気機械式センサから受信された情報を含むようにそのメッセージを作成する作成工程を含んでいることを特徴とする請求項12に記載の通信処理方法。

【請求項18】 メッセージを作成する前記作成工程がビジネスオフィス機器である前記機械の電気機械式センサから受信された情報を含むようにそのメッセージを作成する作成工程を含んでいることを特徴とする請求項17に記載の通信処理方法。

【請求項19】 さらに、前記防護装置を介して前記機械から送られるメッセージのログを作成する作成工程を含んでおり、前記分析工程が、前記セキュリティ装置によって前記機械から受信されたメッセージを前記防護装置を介して発信されるメッセージのログと比較される比較工程を含んでいることを特徴とする請求項1に記載の通信処理方法。

【請求項20】 さらに、前記機械から受信されたメッセージの一つが前記防護装置を介して送られるメッセージのログと合致しない場合に警告を出す警告工程を含んでいることを特徴とする請求項19に記載の通信処理方法。

【請求項21】 さらに、前記機械から受信されたメッセージの一つが前記比較工程で前記防護装置を介して送られるメッセージのログ内に存在していないと判断された場合に、前記防護装置を介しての前記機械からの、さらなる通信を禁止する禁止工程を含んでいることを特徴とする請求項19に記載の通信処理方法。

【請求項22】 メッセージを作成する前記作成工程が前記機械の電気機械式センサから受信された情報を含むようにそのメッセージを作成する作成工程を含んでいることを特徴とする請求項19に記載の通信処理方法。

【請求項23】 メッセージを作成する前記作成工程がビジネスオフィス機器である前記機械の電気機械式センサから受信された情報を含むようにそのメッセージを作成する作成工程を含んでいることを特徴とする請求項22に記載の通信処理方法。

【請求項24】 さらに、前記メッセージを前記防護装置に送信し、さらに前記セキュリティ装置に送信する前に、前記メッセージを暗号化する暗号化工程を含んでおり、前記防護装置に送信する前記送信工程が前記防護装

置に前記暗号化されたメッセージを送信する送信工程を含んでおり、

前記セキュリティ装置に送信する前記送信工程が前記防護装置に前記暗号化されたメッセージを送信する送信工程を含んでおり、

さらに前記方法が、

前記メッセージを前記セキュリティ装置によって解読する解読工程を含んでおり、前記分析工程が解読されたメッセージの内容を分析する分析工程を含んでいることを特徴とする請求項1に記載の通信処理方法。

【請求項25】 さらに、前記解読されたメッセージを復号化する復号化工程を含んでおり、

前記分析工程が、解読され、復号化された前記メッセージの内容を分析する分析工程を含んでいることを特徴とする請求項24に記載の通信処理方法。

【請求項26】 前記分析工程は、前記メッセージの内容が前記データ・センターとの通信を認められている機械からのものであるかどうかを判定する判定工程を含んでいることを特徴とする請求項24に記載の通信処理方法。

【請求項27】 前記分析工程は、前記メッセージの内容が前記データ・センターに送られることを認められている情報のみを含んでいるかどうかを判定する判定工程を含んでいることを特徴とする請求項24に記載の通信制御方法。

【請求項28】 メッセージを作成する前記作成工程が、前記機械の電気機械式センサから受信された情報を含むようにそのメッセージを作成する作成工程を含んでいることを特徴とする請求項24に記載の通信制御方法。

【請求項29】 メッセージを作成する前記作成工程が、ビジネスオフィス機器である前記機械の電気機械式センサから受信された情報を含むようにそのメッセージを作成する作成工程を含んでいることを特徴とする請求項28に記載の通信制御方法。

【請求項30】 メッセージを発生させてそのメッセージをデータ・センターにおくる電気機械式センサを有する機械と、

防護装置と、

セキュリティ装置と、

前記機械、前記防護装置、前記セキュリティ装置および

前記データ・センターを接続する手段と、

前記機械内に配置された、前記データ・センターに送られるべき前記機械の情報を含んだメッセージを作成するための手段と、

前記機械からの前記メッセージを防護装置に送る手段と、

と、

前記メッセージをセキュリティ装置に送る手段と、

前記セキュリティ装置内に配置された、前記メッセージを分析する手段と、を備えたことを特徴とする通信処理

システム。

【請求項31】 前記メッセージを前記セキュリティ装置に送る前記手段が、前記防護装置が受信した前記メッセージを前記セキュリティ装置に送る手段を備えたことを特徴とする請求項30に記載の通信処理システム。

【請求項32】 さらに、前記分析手段が前記メッセージが認められたものでないと判断した場合に、セキュリティ動作を実行する手段を備えたことを特徴とする請求項30に記載の通信処理システム。

【請求項33】 セキュリティ動作を行う前記手段は、前記メッセージが前記防護装置を介して送られることを禁止するための手段を備えたことを特徴とする請求項30に記載の通信処理システム。

【請求項34】 セキュリティ動作を実行する前記手段は、さらなるメッセージが前記防護装置を通じて送られることを禁止する手段を備えたことを特徴とする請求項30に記載の通信処理システム。

【請求項35】 さらに、前記防護装置に送られる前記メッセージを暗号化する手段と、前記セキュリティ装置内で、前記防護装置から受信された暗号化されたメッセージを解読する手段と、を備えたことを特徴とする請求項30に記載の通信処理システム。

【請求項36】 前記防護装置を介して発信されるメッセージをログ内にロギングする手段を備えており、前記分析する手段が、前記セキュリティ装置で受信されたメッセージを前記防護装置を介して送られるメッセージのログと比較する手段を備えたことを特徴とする請求項30に記載の通信処理システム。

【請求項37】 さらに、前記セキュリティ装置で受信されたメッセージを比較する前記手段が、前記防護装置を介して発信されるメッセージの一つが前記セキュリティ装置が受信した対応するメッセージを合致しないと判断した場合に、前記セキュリティ装置に送られたメッセージの一つが前記防護装置を介して発信されるメッセージの対応するものと合致しないことを示す手段を備えたことを特徴とする請求項36に記載の通信処理システム。

【請求項38】 前記メッセージを前記セキュリティ装置に送る前記手段が前記メッセージを前記防護装置の一部である前記セキュリティ装置に送ることを特徴とする請求項30に記載の通信処理システム。

【請求項39】 メッセージを作成する前記手段が、前記機械の前記電気機械式センサから受信された情報を含むようにそのメッセージを作成する手段を備えたことを特徴とする請求項30に記載の通信処理システム。

【請求項40】 メッセージを作成する前記手段が、ビジネスオフィス機器である前記機械の前記電気機械式センサから受信された情報を含むようにそのメッセージを作成する手段を備えたことを特徴とする請求項30に記載

の通信処理システム。

【請求項41】 前記メッセージを前記セキュリティ装置に送るための前記手段が、

前記防護装置からの前記メッセージを前記セキュリティ装置に送る手段を備えており、さらに、前記機械からの前記メッセージを前記セキュリティ装置に送る手段を備えており、

前記分析手段が、

前記セキュリティ装置によって、前記機械からの前記セキュリティ装置により受信された前記メッセージを前記防護装置から前記セキュリティ装置によって受信されたメッセージと比較する手段を備えたことを特徴とする請求項30に記載の通信処理システム。

【請求項42】 さらに、前記メッセージを前記防護装置に送信する前に、前記防護装置に送られるべき前記メッセージを暗号化する手段を備えており、

前記メッセージを前記防護装置から前記セキュリティ装置に送る前記手段が、前記暗号化されたメッセージを送信する手段を備えており、

さらに、該システムが、前記セキュリティ装置によって前記防護装置から受信された前記暗号化メッセージを解読する手段を備えており、

前記比較手段が、前記機械によって受信された前記メッセージを解読されたメッセージと比較する手段を備えたことを特徴とする請求項41に記載の通信処理システム。

【請求項43】 前記メッセージを前記機械から前記セキュリティ装置に送信する前記手段が、前記メッセージを非暗号化形式で送信する手段を備えたことを特徴とする請求項42に記載の通信処理システム。

【請求項44】 さらに、前記防護装置を介して発信されるメッセージをロギングする手段と、

前記セキュリティ装置で受信されたメッセージを前記防護装置を介して送られ、ログされたメッセージと比較する手段と、

を備えたことを特徴とする請求項41に記載の通信処理システム。

【請求項45】 さらに、前記セキュリティ装置で受信されたメッセージを比較する手段が、前記防護装置を介して発信されるメッセージの一つが前記セキュリティ装置によって受信された対応するメッセージに合致しないと判断した場合に、前記セキュリティ装置に送られたメッセージの一つが前記防護装置を通じて送られたメッセージの対応するものと合致しないことを示す警告を出力する手段を備えたことを特徴とする請求項44に記載の通信処理システム。

【請求項46】 メッセージを作成する前記手段が、前記機械の電気機械式センサから受信された情報を含むようにそのメッセージを作成する手段を備えたことを特徴とする請求項42に記載の通信処理システム。

【請求項 47】 メッセージを作成する前記手段が、ビジネスオフィス機器である前記機械の電気機械式センサから受信された情報を含むようにそのメッセージを作成する手段を備えたことを特徴とする請求項 42 に記載の通信処理システム。

【請求項 48】 さらに、機械から前記防護装置を通じて送られるメッセージのログを作成する手段を備えており、

前記分析手段が、前記機械から受信されたメッセージを前記セキュリティ装置によって比較する手段を備えたことを特徴とする請求項 30 に記載の通信処理システム。

【請求項 49】 さらに、前記機械から受信されたメッセージの一つが前記防護装置を介して送られるメッセージのログに対応していない場合に警告を出力する手段を備えたことを特徴とする請求項 48 に記載の通信処理システム。

【請求項 50】 さらに、前記機械から受信されたメッセージの一つが前記比較手段によって前記防護装置を介して送られるメッセージのログに存在していないと判断された場合に、前記機械からのさらなるメッセージが前記防護装置を通じて送られないようにする手段を備えたことを特徴とする請求項 48 に記載の通信処理システム。

【請求項 51】 メッセージを作成する前記手段が、前記機械の電気機械式センサから受信された情報を含むようにそのメッセージを作成する手段を備えたことを特徴とする請求項 48 に記載の通信処理システム。

【請求項 52】 メッセージを作成する前記手段が、ビジネスオフィス機器である前記機械の電気機械式センサから受信された情報を含むようにそのメッセージを作成する手段を備えたことを特徴とする請求項 48 に記載の通信処理システム。

【請求項 53】 さらに、前記メッセージが前記防護装置に送られると同時にセキュリティ装置にも送られる前に、前記メッセージを暗号化する手段と備えており、前記防護装置に送信する前記手段が前記暗号化されたメッセージを前記防護装置に送る手段を備えており、前記セキュリティ装置に送信する手段が前記暗号化されたメッセージを前記防護装置に送信する手段を備えており、さらに該システムが、

前記セキュリティ装置によって前記メッセージを解読する手段を備えており、前記分析手段が解読されたメッセージの内容を分析する手段を備えたことを特徴とする請求項 30 に記載の通信処理システム。

【請求項 54】 さらに、前記解読されたメッセージを復号化する手段を備えており、前記分析手段が、解読され、復号されたメッセージの内容を分析するための手段を備えたことを特徴とする請求項 53 に記載の通信処理システム。

【請求項 55】 前記分析手段が、前記メッセージの内容が前記データ・センターと通信することを認められた機械からのものであるかどうかを判定する手段を備えたことを特徴とする請求項 53 に記載の通信処理システム。

【請求項 56】 前記分析手段が、前記メッセージの内容が前記データ・センターに送られることが認められている情報だけを含んでいるかどうかについて判定する手段を備えたことを特徴とする請求項 53 に記載の通信処理システム。

【請求項 57】 メッセージを作成する前記手段が、前記機械の電気機械式センサから受信した情報を含むように前記メッセージを作成する手段を備えたことを特徴とする請求項 53 に記載の通信処理システム。

【請求項 58】 メッセージを作成する前記手段が、ビジネスオフィス機器である前記機械の電気機械式センサから受信した情報を含むように前記メッセージを作成する手段を備えたことを特徴とする請求項 53 に記載の通信処理システム。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、被モニター装置とモニター装置との間の通信方法、その通信システムおよびコンピュータ・プログラム製品に関し、より詳細には、接続通信モードと無接続通信モードを用いた被モニター装置とモニター装置との間におけるリモート・モニタリング、診断、および制御に関し、さらに具体的には、複写機やプリンタ、そしてファクシミリ装置等のビジネスオフィス機器のモニタリング、制御、および診断に関するものである。

【0002】本発明はさらに、発信無接続通信が確実に承認され、かつその秘密が保持されるようにすることに関するものである。

【0003】

【従来の技術】本発明に関連する技術としては、『多重通信フォーマットを用いる機械を制御し、それと通信するための方法およびシステム』と題する 1996 年 3 月 29 日出願の米国特許出願 08/624,228、『接続および無接続通信モードを用いる機械の診断、制御のための方法およびシステム』と題する 1995 年 6 月 5 日出願の米国特許出願 08/463,002、および、現在放棄されている、1990 年 7 月 6 日出願米国特許出願 07/549,278 の継続出願で、現在放棄されている 1992 年 6 月 19 日出願米国特許出願 07/902,462 の継続出願で、現在米国特許 5,412,779 とされている 1994 年 7 月 28 日出願で『ビジネスオフィス機器の制御およびそれらとの通信のための方法および装置』と題する米国特許出願 08/282,168 の継続出願である 1995 年 4 月 24 日出願で、『ビジネスオフィス機器の制御およびそれらとの通信の

ための方法および装置』と題する現在米国特許 5、537、554 である米国特許出願 08/426、679 の継続出願であり、『ビジネスオフィス機器の制御および、それらと通信のための方法および装置』と題される現在米国特許 5、544、289 である 1995 年 6 月 6 日出願の米国特許出願 08/473、780 の継続出願であり、1995 年 11 月 22 日出願の米国特許出願 08/562、192 の継続出願である『ビジネスオフィス機器の制御および、それらとの通信のための方法および装置』と題する 1996 年 8 月 15 日出願の米国特許出願 08/x x x、x x x がある。なお、これら資料における開示は本明細書に引例として組み込まれている。

【0004】

【発明が解決しようとする課題】しかしながら、上記米国特許 5、412、779 はリモート診断装置によるビジネスオフィス機器の制御について開示しているものの、このシステムおよびビジネスオフィス機器等の装置を制御する他の公知のシステムにおいては、その装置（被モニター装置）とリモート診断装置（モニター装置）との間で、接続および接続通信モードでの通信の利用が必要であるため、このような装置とリモート診断装置との間の専用通信接続の利用は、インターネットを使用した場合と比較してより経費がかかるという問題点があった。

【0005】一方、インターネットにおいては、インターネットを用いたある種の通信は速度が遅かったり、遅れたりする欠陥を有しており、またインターネットは安全な送信モードではない（つまり、他者によってモニターされる場合がある）という問題を有している。さらに、インターネットから設置された装置への接続モード・アクセスが、ファイアーウォール（fire wall）等のセキュリティ・ブロックによって不可能な場合もあるという問題点もあった。

【0006】ところが、インターネットによる接続モードでの通信が遅い等の問題があったとしても、本発明者はインターネットが一部の装置にとって適した通信媒体を提供できることを見出している。

【0007】本発明は上記に鑑みてなされたものであって、被モニター装置とモニター装置（リモート診断装置）との間の無接続通信を可能にするを一つの目的とする。

【0008】また、本発明は上記に鑑みてなされたものであって、発信無接続通信が確実に承認され、かつその秘密が保持されるようにする方法およびシステムを提供することを他の目的とする。

【0009】これら、およびその他の目的はファクシミリ装置、複写機、あるいはプリンタなどを含むビジネスオフィス機器からの発信通信をモニターする方法およびシステムによって達成される。

【0010】インターネットを通じて上記ビジネスオフィス機器からそれらビジネスオフィス機器のステータスおよびパラメータをモニターするデータ・センターに送られる、これらのメッセージはインターネットを通じて防護装置に送られる前に、好ましくはローカル・エリア・ネットワークを通じてセキュリティ・センターに送られる。このセキュリティ・センターは送信される情報が確実に受け入れられ、許可された送信先に送られるようにするために上記情報をモニターする。

【0011】セキュリティ・センターによって受信されたメッセージは暗号化されている場合と、暗号化されていない場合とがある。メッセージが暗号化されている場合は、まずそのメッセージを上記セキュリティ・センターで解読しなければならない。その後、そのメッセージ内のデータが分析される。二値形式の場合もある発信メッセージの内容を判定するために、上記セキュリティ・センターでソフトウェア・プログラムが用いられる場合もある。

【0012】ソフトウェア・プログラムが必要なのは、発信メッセージが 2 つの機械間を送信され、人間ではその内容が迅速に理解できないからである。発信メッセージをモニターすることによって、特定の機械のデータだけが発信され、ビジネスオフィス機器からのメッセージのように偽装されている可能性のある他のデータは送信されないようにすることができる。

【0013】さらに、防護装置を通じてインターネットに送られる発信メッセージのログが保存される。このログはビジネスオフィス機器からの発信メッセージのすべてがセキュリティ・センターによって確実に受信されるようにするために、セキュリティ・センターによって受信されたメッセージと比較される。

【0014】そのメッセージの送信が受け入れ可能であると判断された場合、暗号化形式のメッセージがインターネットを通じて、好ましくは電子メール・メッセージの形式で送られるが、他のタイプのメッセージおよび通信メディアを用いることも可能である。望ましい場合、一つの機械の履歴をモニターできるようにするために、そして過去の秘密漏洩について調べることができるようにするために、上記セキュリティ・グループは発信メッセージを記憶し、保管する。

【0015】

【課題を解決するための手段】上記の目的を達成するために、請求項 1 に係る通信処理方法にあつては、電気機械式センサを有する機械からデータ・センターへの通信を処理する通信処理方法において、前記データ・センターに送られる情報を含んだメッセージを作成する作成工程と、前記メッセージを前記機械から防護装置に送信する送信工程と、前記メッセージをセキュリティ装置に送信する送信工程と、前記セキュリティ装置によって前記メッセージを分析する分析工程と、を含んでいるもので

ある。る通信処理方法。

【0016】請求項2に係る通信処理方法にあつては、さらに、前記メッセージを前記セキュリティ装置に送信する送信工程が、前記メッセージを前記防護装置によって受信されたメッセージを前記セキュリティ装置に送信する送信工程を含んでいるものである。

【0017】請求項3に係る通信処理方法にあつては、さらに、前記分析工程で前記メッセージが認められたメッセージでないと判定された場合にセキュリティ動作を実行するセキュリティ工程を含んでいるものである。

【0018】請求項4に係る通信処理方法にあつては、さらに、セキュリティ動作を実行するセキュリティ工程が、前記防護装置を通過して来るメッセージを禁止する禁止工程を含んでいるものである。

【0019】請求項5に係る通信処理方法にあつては、さらに、セキュリティ動作を実行するセキュリティ工程が、前記防護装置を通過して来る、さらなるメッセージを禁止する禁止工程を含んでいるものである。

【0020】請求項6に係る通信処理方法にあつては、さらに、前記防護装置に送られるメッセージを、前記防護装置に送られる前に暗号化する暗号化工程と、前記防護装置から受信された暗号化されたメッセージをセキュリティ装置により解読する解読工程と、を含んでいるものである。

【0021】請求項7に係る通信処理方法にあつては、さらに、前記防護装置を通じて発信されるメッセージをログ内にロギングするロギング工程を含んでおり、前記分析工程が、前記セキュリティ装置で受信されるメッセージを前記防護装置を通じて発信されるメッセージのログと比較する比較工程を含んでいるものである。

【0022】請求項8に係る通信処理方法にあつては、さらに、前記セキュリティ装置で受信されたメッセージを比較する比較工程で、前記防護装置を通じて発信されるメッセージの一つが、セキュリティ装置によって受信された対応するメッセージと合致していない場合に、前記セキュリティ装置で受信されたメッセージの一つが前記防護装置を通じて発信されるメッセージの対応するものと合致しないことを示す警告を出力する警告工程を含んでいるものである。

【0023】請求項9に係る通信処理方法にあつては、前記メッセージをセキュリティ装置に送信する送信工程で、前記防護装置の一部であるセキュリティ装置にそのメッセージを送信する送信工程を含んでいるものである。

【0024】請求項10に係る通信処理方法にあつては、メッセージを作成する作成工程が、前記機械の電気機械式センサから受信された情報を含むメッセージを作成する作成工程を含んでいるものである。

【0025】請求項11に係る通信処理方法にあつては、メッセージを作成する作成工程が、ビジネスオフィ

ス機器である前記機械の電気機械式センサから受信された情報を含むメッセージを作成する作成工程を含んでいるものである。

【0026】請求項12に係る通信処理方法にあつては、前記メッセージを前記セキュリティ装置に送信する送信工程が、前記メッセージを前記防護装置から前記セキュリティ装置に送信する送信工程と、前記メッセージを前記機械から前記セキュリティ装置に送信する送信工程と、を含んでおり、前記分析工程が、前記セキュリティ装置によって、前記セキュリティ装置が前記機械から受信した前記メッセージを、前記防護装置から前記セキュリティ装置が受信したメッセージと比較する比較工程を含んでいるものである。

【0027】請求項13に係る通信処理方法にあつては、さらに、前記メッセージを前記防護装置に送信する前に、その防護装置に送信されるメッセージを暗号化する暗号化工程と、前記防護装置からのメッセージを前記セキュリティ装置に送信する送信工程がそのメッセージを暗号化する暗号化工程と、さらに、前記セキュリティ装置によって、前記防護装置から受信された暗号化されたメッセージを解読する解読工程と、前記機械から受信された前記メッセージを解読されたメッセージと比較する比較工程と、を含んでいるものである。

【0028】請求項14に係る通信処理方法にあつては、前記メッセージを前記機械から前記セキュリティ装置に送信する送信工程が、前記メッセージを非暗号化形式で送信する送信工程を含んでいるものである。

【0029】請求項15に係る通信処理方法にあつては、さらに、前記防護装置から発信されるメッセージをロギングするロギング工程と、前記セキュリティ装置で受信されたメッセージを前記防護装置を介して送信され、ログされたメッセージと比較する比較工程と、を含んでいるものである。

【0030】請求項16に係る通信処理方法にあつては、さらに、前記セキュリティ装置で受信されたメッセージを比較する比較工程で、前記防護装置を介して送られるメッセージの一つが前記セキュリティ装置によって受信されたメッセージと合致しないと判断された場合に、前記セキュリティ装置に送信されたメッセージの一つが前記防護装置を通じて発信されるメッセージの対応するものと合致しないことを示す警告を出す警告工程を含んでいることを特徴とする請求項15に記載の通信処理方法。

【0031】請求項17に係る通信処理方法にあつては、メッセージを作成する前記作成工程が前記機械の電気機械式センサから受信された情報を含むようにそのメッセージを作成する作成工程を含んでいるものである。

【0032】請求項18に係る通信処理方法にあつては、メッセージを作成する前記作成工程がビジネスオフィス機器である前記機械の電気機械式センサから受信さ

れた情報を含むようにそのメッセージを作成する作成工程を含んでいるものである。

【0033】請求項19に係る通信処理方法にあっては、さらに、前記防護装置を介して前記機械から送られるメッセージのログを作成する作成工程を含んでおり、前記分析工程が、前記セキュリティ装置によって前記機械から受信されたメッセージを前記防護装置を介して発信されるメッセージのログと比較される比較工程を含んでいるものである。

【0034】請求項20に係る通信処理方法にあっては、さらに、前記機械から受信されたメッセージの一つが前記防護装置を介して送られるメッセージのログと合致しない場合に警告を出す警告工程を含んでいるものである。

【0035】請求項21に係る通信処理方法にあっては、さらに、前記機械から受信されたメッセージの一つが前記比較工程で前記防護装置を介して送られるメッセージのログ内に存在していないと判断された場合に、前記防護装置を介しての前記機械からの、さらなる通信を禁止する禁止工程を含んでいるものである。

【0036】請求項22に係る通信処理方法にあっては、メッセージを作成する前記作成工程が前記機械の電気機械式センサから受信された情報を含むようにそのメッセージを作成する作成工程を含んでいるものである。

【0037】請求項23に係る通信処理方法にあっては、メッセージを作成する前記作成工程がビジネスオフィス機器である前記機械の電気機械式センサから受信された情報を含むようにそのメッセージを作成する作成工程を含んでいるものである。

【0038】請求項24に係る通信処理方法にあっては、さらに、前記メッセージを前記防護装置に送信し、さらに前記セキュリティ装置に送信する前に、前記メッセージを暗号化する暗号化工程を含んでおり、前記防護装置に送信する前記送信工程が前記防護装置に前記暗号化されたメッセージを送信する送信工程を含んでおり、前記セキュリティ装置に送信する前記送信工程が前記防護装置に前記暗号化されたメッセージを送信する送信工程を含んでおり、さらに前記方法が、前記メッセージを前記セキュリティ装置によって解読する解読工程を含んでおり、前記分析工程が解読されたメッセージの内容を分析する分析工程を含んでいるものである。

【0039】請求項25に係る通信処理方法にあっては、さらに、前記解読されたメッセージを復号化する復号化工程を含んでおり、前記分析工程が、解読され、復号化された前記メッセージの内容を分析する分析工程を含んでいるものである。

【0040】請求項26に係る通信処理方法にあっては、前記分析工程は、前記メッセージの内容が前記データ・センターとの通信を認められている機械からのものであるかどうかを判定する判定工程を含んでいるもので

ある。

【0041】請求項27に係る通信処理方法にあっては、前記分析工程は、前記メッセージの内容が前記データ・センターに送られることを認められている情報のみを含んでいるかどうかを判定する判定工程を含んでいるものである。

【0042】請求項28に係る通信処理方法にあっては、メッセージを作成する前記作成工程が、前記機械の電気機械式センサから受信された情報を含むようにそのメッセージを作成する作成工程を含んでいるものである。

【0043】請求項29に係る通信処理方法にあっては、メッセージを作成する前記作成工程が、ビジネスオフィス機器である前記機械の電気機械式センサから受信された情報を含むようにそのメッセージを作成する作成工程を含んでいるものである。

【0044】また、請求項30に係る通信処理システムにあっては、メッセージを発生させてそのメッセージをデータ・センターにおくる電気機械式センサを有する機械と、防護装置と、セキュリティ装置と、前記機械、前記防護装置、前記セキュリティ装置および前記データ・センターを接続する手段と、前記機械内に配置された、前記データ・センターに送られるべき前記機械の情報を含んだメッセージを作成するための手段と、前記機械からの前記メッセージを防護装置に送る手段と、前記メッセージをセキュリティ装置に送る手段と、前記セキュリティ装置内に配置された、前記メッセージを分析する手段と、を備えたものである。

【0045】請求項31に係る通信処理システムにあっては、前記メッセージを前記セキュリティ装置に送る前記手段が、前記防護装置が受信した前記メッセージを前記セキュリティ装置に送る手段を備えたものである。

【0046】請求項32に係る通信処理システムにあっては、さらに、前記分析手段が前記メッセージが認められたものでないと判断した場合に、セキュリティ動作を実行する手段を備えたものである。

【0047】請求項33に係る通信処理システムにあっては、セキュリティ動作を行う前記手段は、前記メッセージが前記防護装置を介して送られることを禁止するための手段を備えたものである。

【0048】請求項34に係る通信処理システムにあっては、セキュリティ動作を実行する前記手段は、さらなるメッセージが前記防護装置を通じて送られることを禁止する手段を備えたものである。

【0049】請求項35に係る通信処理システムにあっては、さらに、前記防護装置に送られる前記メッセージを暗号化する手段と、前記セキュリティ装置内で、前記防護装置から受信された暗号化されたメッセージを解読する手段と、を備えたものである。

【0050】請求項36に係る通信処理システムにあって

ては、前記防護装置を介して発信されるメッセージをログ内にロギングする手段を備えており、前記分析する手段が、前記セキュリティ装置で受信されたメッセージを前記防護装置を介して送られるメッセージのログと比較する手段を備えたものである。

【0051】請求項37に係る通信処理システムにあつては、さらに、前記セキュリティ装置で受信されたメッセージと比較する前記手段が、前記防護装置を介して発信されるメッセージの一つが前記セキュリティ装置で受信した対応するメッセージを合致しないと判断した場合に、前記セキュリティ装置に送られたメッセージの一つが前記防護装置を介して発信されるメッセージの対応するものと合致しないことを示す手段を備えたものである。

【0052】請求項38に係る通信処理システムにあつては、前記メッセージを前記セキュリティ装置に送る前記手段が前記メッセージを前記防護装置の一部である前記セキュリティ装置に送るものである。

【0053】請求項39に係る通信処理システムにあつては、メッセージを作成する前記手段が、前記機械の前記電気機械式センサから受信された情報を含むようにそのメッセージを作成する手段を備えたものである。

【0054】請求項40に係る通信処理システムにあつては、メッセージを作成する前記手段が、ビジネスオフィス機器である前記機械の前記電気機械式センサから受信された情報を含むようにそのメッセージを作成する手段を備えたものである。

【0055】請求項41に係る通信処理システムにあつては、前記メッセージを前記セキュリティ装置に送るための前記手段が、前記防護装置からの前記メッセージを前記セキュリティ装置に送る手段を備えており、さらに、前記機械からの前記メッセージを前記セキュリティ装置に送る手段を備えており、前記分析手段が、前記セキュリティ装置によって、前記機械からの前記セキュリティ装置により受信された前記メッセージを前記防護装置から前記セキュリティ装置によって受信されたメッセージと比較する手段を備えたものである。

【0056】請求項42に係る通信処理システムにあつては、さらに、前記メッセージを前記防護装置に送信する前に、前記防護装置に送られるべき前記メッセージを暗号化する手段を備えており、前記メッセージを前記防護装置から前記セキュリティ装置に送る前記手段が、前記暗号化されたメッセージを送信する手段を備えており、さらに、該システムが、前記セキュリティ装置によって前記防護装置から受信された前記暗号化メッセージを解読する手段を備えており、前記比較手段が、前記機械によって受信された前記メッセージを解読されたメッセージと比較する手段を備えたものである。

【0057】請求項43に係る通信処理システムにあつては、前記メッセージを前記機械から前記セキュリティ

装置に送信する前記手段が、前記メッセージを非暗号化形式で送信する手段を備えたものである。

【0058】請求項44に係る通信処理システムにあつては、さらに、前記防護装置を介して発信されるメッセージをロギングする手段と、前記セキュリティ装置で受信されたメッセージを前記防護装置を介して送られ、ログされたメッセージと比較する手段と、を備えたものである。

【0059】請求項45に係る通信処理システムにあつては、さらに、前記セキュリティ装置で受信されたメッセージと比較する手段が、前記防護装置を介して発信されるメッセージの一つが前記セキュリティ装置によって受信された対応するメッセージに合致しないと判断した場合に、前記セキュリティ装置に送られたメッセージの一つが前記防護装置を通じて送られたメッセージの対応するものと合致しないことを示す警告を出力する手段を備えたものである。

【0060】請求項46に係る通信処理システムにあつては、メッセージを作成する前記手段が、前記機械の電気機械式センサから受信された情報を含むようにそのメッセージを作成する手段を備えたものである。

【0061】請求項47に係る通信処理システムにあつては、メッセージを作成する前記手段が、ビジネスオフィス機器である前記機械の電気機械式センサから受信された情報を含むようにそのメッセージを作成する手段を備えたものである。

【0062】請求項48に係る通信処理システムにあつては、さらに、機械から前記防護装置を通じて送られるメッセージのログを作成する手段を備えており、前記分析手段が、前記機械から受信されたメッセージを前記セキュリティ装置によって比較する手段を備えたものである。

【0063】請求項49に係る通信処理システムにあつては、さらに、前記機械から受信されたメッセージの一つが前記防護装置を介して送られるメッセージのログに対応していない場合に警告を出力する手段を備えたものである。

【0064】請求項50に係る通信処理システムにあつては、さらに、前記機械から受信されたメッセージの一つが前記比較手段によって前記防護装置を介して送られるメッセージのログに存在していないと判断された場合に、前記機械からのさらなるメッセージが前記防護装置を通じて送られないようにする手段を備えたものである。

【0065】請求項51に係る通信処理システムにあつては、メッセージを作成する前記手段が、前記機械の電気機械式センサから受信された情報を含むようにそのメッセージを作成する手段を備えたものである。

【0066】請求項52に係る通信処理システムにあつては、メッセージを作成する前記手段が、ビジネスオフ

イス機器である前記機械の電気機械式センサから受信された情報を含むようにそのメッセージを作成する手段を備えたものである。

【0067】請求項53に係る通信処理システムにおいては、さらに、前記メッセージが前記防護装置に送られると同時にセキュリティ装置にも送られる前に、前記メッセージを暗号化する手段と備えており、前記防護装置に送信する前記手段が前記暗号化されたメッセージを前記防護装置に送る手段を備えており、前記セキュリティ装置に送信する手段が前記暗号化されたメッセージを前記防護装置に送信する手段を備えており、さらに該システムが、前記セキュリティ装置によって前記メッセージを解読する手段を備えており、前記分析手段が解読されたメッセージの内容を分析する手段を備えたものである。

【0068】請求項54に係る通信処理システムにおいては、さらに、前記解読されたメッセージを復号化する手段を備えており、前記分析手段が、解読され、復号されたメッセージの内容を分析するための手段を備えたものである。

【0069】請求項55に係る通信処理システムにおいては、前記分析手段が、前記メッセージの内容が前記データ・センターと通信することを認められた機械からのものであるかどうかを判定する手段を備えたものである。

【0070】請求項56に係る通信処理システムにおいては、前記分析手段が、前記メッセージの内容が前記データ・センターに送られることが認められている情報だけを含んでいるかどうかについて判定する手段を備えたものである。

【0071】請求項57に係る通信処理システムにおいては、メッセージを作成する前記手段が、前記機械の電気機械式センサから受信した情報を含むように前記メッセージを作成する手段を備えたものである。

【0072】請求項58に係る通信処理システムにおいては、メッセージを作成する前記手段が、ビジネスオフィス機器である前記機械の電気機械式センサから受信した情報を含むように前記メッセージを作成する手段を備えたものである。

【0073】

【発明の実施の形態】以下、この発明に係る通信処理方法および通信処理システムの実施の形態を、図面を参照して詳細に説明する。

【0074】なお、本発明において利用が可能な安価な接続通信モードはインターネットである。ただし、その装置内で緊急の注意を要するような状態が発生した場合、無接続通信モードは不適切な場合がある。こうした場合に使用される通信モードは通常の電話あるいはISDN回線を用いた接続モードであろう。

【0075】図1は、複写機1、操作パネル2および遠

隔診断ステーション3を含む本発明の好適な実施の形態を示す。しかしながら、本発明は複写機に限定されず、以下に説明する手段を有するプリンタ或いはファクシミリのような他のビジネス機器にも適用できる。

【0076】以下の説明において、図1に示す目標装置は複写機1である。目標装置である複写機1はその寿命の間変わらない静的状態データ1107、例えばモデル番号、シリアル番号、モデル特性等を記憶する手段を含む。また、目標装置である複写機1はROMバージョン、オプション構成のような装置の寿命の間めったに変わらない半静的状態データ1106を記憶する手段も含む。

【0077】さらに、目標装置である複写機1は、トレーにおける記録紙の状態、オイル、トナー、プリント数、受光素子の感度、記録紙の通路および位置等のような装置の機械的状态によって変わる動的状態データ1105を記憶する手段を有する。装置の動的状態を記憶するために、目標装置である複写機1は該複写機1の状態を監視する監視プロセス1104を含む。システム全体の動作はシステム制御プロセス1102によって統制動作される。

【0078】電源を入れると、システム制御プロセス1102は目標装置である複写機1を準備させるのみならず、最初に物理的接続をチェックした後、以下に説明する手段で通信を確立することによって附属装置との通信を確立する。

【0079】複写機1は、使用者が操作パネル2を介して幾つかの機能を特定するまでアイドル状態にある。しかしながら、アイドル時間の間、システム制御プロセス1102によってその状態を連続的に監視する。異常状態が検出されると、システム制御プロセス1102はデータを通信プロセス1101に送り、そのデータをコード化してコード化データを通信ライン1012を介して操作パネル2に送る。通信プロセス1201は確認応答信号を送り、データを解読してそれをシステム制御プロセス1202へ送る。システム制御プロセス1202は複写機1の状態をディスプレイプロセス1204を介して通知する。

【0080】遠隔診断ステーションの通信ライン1013が接続されると、システム制御プロセス1102はメッセージを送り、遠隔診断ステーション3に注意を与えてステーション3に異常状態を知らせる。

【0081】入力プロセス1203は使用者からの入力を受けてそれをシステム制御プロセス1202へ送り、該システム制御プロセスはつぎにその入力をディスプレイプロセス1204を介してそのまま戻す（エコー・バック）ので、使用者は彼／彼女（使用者）の入力をフィードバックして得ることができる。使用者からのデータはつぎに通信プロセス1201においてコード化される。このコード化されたデータはつぎにライン1012

を介して複写機へ送られる。

【0082】通信プロセス1101はつぎに通信プロセス1201へ確認応答信号を送り、その受けたデータを解読し、解読したデータをシステム制御プロセス1102へ送る。実際の複写処理中、シーケンスプロセス1103は時限要求に従って事象を配列する。遠隔診断ステーション3は通信ライン1013を介して複写機1に接続される。そのライン1013は電話線、RS232ライン或いはその他の適当な通信手段とすることができる。通信プロセス1301は複写機1の通信プロセス1101および操作パネル20の通信プロセス1201と同様に操作する。

【0083】診断プロセス1302は、受け取る回答とデータベース1303に記憶されているデータに基づいて複写機1と対話的に交信できるインテリジェント（知能）プロセスである。

【0084】図2は本発明を実行するために利用されるハードウェアの特徴を示す。複写機1、操作パネル2および遠隔診断ステーション3は全てバス4、5および6を有し、それらはそれぞれ中央処理装置2111、2211および2311に接続している。モデルに依存して、バスはさらに多くのユニットを有する。センサユニット2113は、記録紙トレイ、電圧および紙の通路のような動的データとして記憶されなければならない目標装置の機能的状態を検出する。

【0085】記憶装置2112は静的状態のデータ1107を（ROMのような）固定記憶として保持する。記憶装置2115は半静的状態のデータ1106をEEPROMのような電力を必要としない交換可能な記憶装置或いは低電力を使用しバッテリーによってサポートできる（CMOSRAMのような）交換可能な記憶装置に記憶する。記憶装置2116は動的状態のデータを電力を必要としない或いは低電力を使用したバッテリーによってサポートできる交換可能な記憶装置に記憶する。

【0086】ディスプレイおよび入力ユニット2213は入力キーおよびライトとLCD（液晶表示装置）のようなディスプレイを制御する。ディスクユニット2313はデータベースを保持する。通信ライン1013が規則的に接続されなかったり、診断が必要となきのみ接続する場合には、インターフェースユニット2114は、物理的接続の機械的手段に起因する中断のようなことを、ライン1013が接続されている中央処理装置2111に知らせる手段を有する。

【0087】図3は本発明による符号化の好適な実施の形態を示す。しかしながら、ASN. 1（1987）のような他のエンコーディング（符号化）も使用することができる。図3における符号化スキーマはタイプ、長さおよび値（TLV）符号化の送信からなる。タイプのビット7は0にセットされるが、長さのビット7は1にセットされる。値はいずれかのビットの組合せをとること

ができる。

【0088】符号化は2進法であってデータ通信の長さを節約する。情報フィールドを組み合わせることによって、120タイプ（4つの情報×30タイプ）まで定義することができる。タイプを拡張する1つの方法は全ての低い5ビットを1にセットすることである。この拡張のターミネータは00Hの2つのバイトである。情報フィールドにおいて複合を使用することにより、1つ以上の情報を以下のように送ることができる。

010 ××××× L1 T2 L2 V2 T3 L3 V3

但し、L1はT2～V3のバイトの長さ、L2はV2のバイトの長さ、L3はV3のバイトの長さである。複合は2つに限定されない。

【0089】つぎの表1はタイプおよび値のコードを示す。これらのコードは説明として示すのであって、実際の実行は用途によって変わる。

【0090】

【表1】

情報	タイプ	内 容
00	1	確認
00	2	識別
00	3	コピーの番号
00	4	開始
00	5	終了
00	6	問合せ
00	7	報告
00	8	アドレス内容の報告
00	9	パラメータの報告
01	1	理解否定コマンド
10	1	複合確認
11	1	ジャム

識 別 値

1	複写機
2	操作パネル
3	診断

問 合 せ 値

1	同一
2	モデル

【0091】図4は電源を入れた後、図1あるいは図2の複写機1と操作パネル2間の通信の確立を示す。複写機1と操作パネル2は共にパワーオン・リセット・シーケンスで通じる。ステップ1において、操作パネル2はリセットを終了し、その割り当てられた値を複写機1へ送る。

【0092】しかしながら、複写機1はリセットで忙しく、インターフェースユニット2114を介してデータを入手できない。ステップ2において、複写機1は準備完了し割り当てられた値を操作パネル2へ送る。ステッ

ブ3はパネル2から複写機1への確認を示す。好適実施例において、受信側は受信したタイプの確認を戻さなければならない。

【0093】図4のステップ4は最初の識別が中断して別の試みを行うべきであることを示す。ステップ5は接続が確立されたことを示す。ステップ6は特定されたコピー枚数の例を示す。ステップ7における確認はコピー枚数（ここでは、3コピー）を表す。ステップ8は複写処理シーケンスの開始を示し、ステップ9は対応する確認を示す。ステップ10は記録紙ジャムの通信を示し、ステップ工程11はその記録紙ジャムの対応する確認を示す。

【0094】図5は図1と図2の診断ステーション3と複写機1間の接続の確立過程を示す。図5はライン4および6で複合情報フィールドの使用を示す。この複合が使用されないと、ライン10～12のような通信が必要である。

【0095】図5のステップ1は診断の識別を示し、ステップ2はその識別の確認を示す。ステップ3は識別の問合せを示し、ステップ4は複合確認を示す。ステップ5はモデルの識別について問合せをし、ステップ6は対応する確認である。ステップ7はパラメータの報告を質問し、説明としてステップ8はコマンドが理解されないことを示す。ステップ9はアドレスの報告を示し、ステップ10、11および12はそれぞれ確認、報告および確認を示す。

【0096】本発明の被モニター装置（診断、制御される装置）は、従来のローカル・エリア・ネットワーク（LAN）に接続されている場合もある。また、このローカル・エリア・ネットワークは、安全目的のためのファイアーウォール（防護装置）を介してインターネットに接続することができる。

【0097】詳細は後述するが、本発明において、被モニター装置が最初にそのネットワークに接続されると、その装置の名称およびアドレスがメール・サーバとその装置に、その施設の一部としてのシステム・アドミニストレータによって登録される。これによって、入ってくるインターネット電子メールがメール・サーバによってその装置に導かれる。加えて、その装置の存在を登録するために、例えば、インターネット電子メールを介して無接続メッセージがモニター装置（リモート装置）に送信される。

【0098】本発明はさらに、モニター装置（リモート装置）がその装置の能力を知ることができるように被モニター装置の型式、構成および性能に関する情報を含む装置（または複数の装置）の情報を有しているデータベースを含む。このデータベースは、それら装置の操作特性および信頼性に関する情報に迅速かつ効率的にアクセスできるように、サービス・グループ、マーケティング・グループ、製造グループ、そしてエンジニアリング・

グループ等異なったグループ間で共用されるものである。

【0099】図6は、様々な装置とそれらの装置の動作をモニタリング、診断および制御するためのコンピュータを有したネットワークシステムを有している。具体的には、後述する3つのビジネスオフィス機器（被モニター装置）を、インターネットを介してコンピュータおよびデータベースから成るネットワークに接続した例を示している。なお、図中、同じ参照番号は同じ部品、または対応する部品を示しておく。

【0100】図において、最初のネットワーク17は、コンピュータ・ワークステーション16、18、20および22に接続されたローカル・エリア・ネットワーク（LAN）である。これらのワークステーションは、IBMパーソナル・コンピュータ互換機、ユニックスに基づくコンピュータ、あるいはアップル・マッキントッシュ等どんなものであってもよい。なお、これらのワークステーション16、18、20および22や、後述するワークステーションが必要に応じて本発明のモニター装置の役割を果たす。

【0101】また、ネットワーク17には、デジタル複写機24、ファクシミリ装置28、およびプリンタ32が接続されている。これらデジタル複写機24、ファクシミリ装置28、およびプリンタ32は以下の記述においてビジネスオフィス機器あるいは被モニター装置として記載するが、他のタイプの装置あるいはモニターされる装置を用いてもよい。また、ファクシミリ・サーバー（図示せず）をネットワーク17に接続してもよいし、電話やISDN接続を用いてもよい。

【0102】ネットワーク17に接続されているデジタル複写機24、ファクシミリ装置28およびプリンタ32に加えて、これらの被モニター装置は従来の電話および／またはISDN接続26、30および34を含んでもよい。以下に説明するように、ビジネスオフィス機器（または他のビジネス装置）24、28および32は、モニター装置と称されるリモート・モニタリング、診断および制御ステーション（ステーションとは、端末装置またはデータ処理装置を示す）と、ネットワーク17または直接の電話またはISDN接続経由でインターネットを通じて交信する。

【0103】図6で、インターネットは参照番号10で示されている。インターネット10は、12A～12Iで示される複数の相互接続コンピュータを有している。インターネットを通じて交信する方法は、NIC、DDN、MILまたはFTP NICS、SRI、COMでFTPによって得られる資料を通じて知ることができる。

【0104】TCP/IP関連通信は、例えば“TCP/IP Illustrated” Vol. 1, The Protocols, by Stevens,

from Addison-Wesley Publishing Company、1994に述べられている。

【0105】インターネットは多くの人や組織がアクセスできるネットワークであるからといって、安全であるとは考えることができない。したがって、インターネットを通じて送信されるメッセージは、その秘密を護ために暗号化される必要がある。本発明で用いることが可能な暗号化のメカニズムは知られているし、市販もされている。

【0106】例えば、ユニックス・オペレーティング・システムで使用するためにはSun Microsystems社からCライブラリ機能であるcrypt()を購入することができる。また、その他の暗号化・複合化のルーチンも知られているし、市販もされている。

【0107】コンピュータ・ネットワークをインターネットに接続する際に用いられる追加的な安全手段は、ファイアーウォール(firewall)として知られている防護装置である。この装置は認められたコンピュータだけがインターネットを経由でネットワークや他のコンピュータにアクセスできるようにするものである。ファイアーウォールは公知の市販されている装置で、例えば、Sun Microsystems社のSunScreen等がある。

【0108】図6で、防護装置14がインターネット10とネットワーク17との間に接続されている。同様に、防護装置50がインターネット10とネットワーク52との間に接続されている。また、防護装置40がインターネット10とワークステーション42との間に接続されている。

【0109】ネットワーク52は従来のネットワークで、複数のワークステーション56、62、68および74を含んでいる。これらのワークステーションは一つの会社内の、マーケティング、製造、デザイン・エンジニアリング、および顧客サービス部門等異なった部門に設置されていてもよい。

【0110】ネットワーク52経由で接続されているワークステーションに加えて、ネットワーク52に直接接続されていないワークステーション42がある。ディスク46に保存されているデータベースの情報はインターネットを通じて、ネットワーク52に直接接続されたワークステーションにより、適切な暗号化および手順を用いることにより共用することができる。

【0111】また、ワークステーション42は電話回線および/またはISDN回線44との直接接続を含んでおり、ディスク46内のデータベースはその電話回線あるいはISDN回線を通じてアクセスすることも可能である。

【0112】ビジネスオフィス機器24、28、32の

情報は、ディスク46、54、58、64、70、76に保存されている一つ以上のデータベースに保存されている可能性がある。顧客サービス、マーケティング、製造、エンジニアリングの各部門はそれぞれ独自のデータベースを持っていたり、また一つ以上の部門とデータベースを共用したりしている場合がある。

【0113】データベースを保存するために利用されるそれぞれのディスクは、ハード・ディスクや光ディスクのような不揮発性メモリである。例えば、ディスク64にはマーケティング・データベースが入っており、ディスク58には製造データベース、ディスク70にはエンジニアリング・データベース、またディスク76には顧客サービス・データベースがそれぞれ入っている。またそれらの代わりに、ディスク54と46とには上記データベースが一つ以上保存される。

【0114】ワークステーション56、62、68、74、42がインターネットに接続されていることに加えて、これらのワークステーションには、モニター、診断および/または制御される装置(被モニター装置)に対して安全な接続を提供する電話回線やISDN回線(図中に、60、66、72、80、44で示す)への接続も含まれている。さらに、インターネットや電話回線、あるいはISDN回線の一つが正常に動作しなければ、その内の他の一つを自動的に通信用に利用することが可能である。

【0115】本発明の重要な特徴は、装置の診断や制御のために、装置(被モニター装置)とコンピュータ(モニター装置)間で無接続通信モードの接続および装置を用いることである。George McDanielによるThe IBM Dictionary of Computing(1994年)において、無接続通信モードとは、ソース・サービス・アクセス・ポイントからの単一データ単位を接続なしに一つ以上のサービス・アクセス・ポイントの送信先へ送信することであると定義されている。

【0116】また、IBM Dictionaryは、接続通信モードとは、いくつかのデータをソース・サービス・アクセス・ポイントから接続を介して一つ以上のサービス・アクセス・ポイントの送信先へ送信することであると定義している。

【0117】接続はデータ転送以前に行われ、データ転送後に開放される。さらに、操作の接続通信モードと無接続通信モードに関する情報は、William StallingsによるThe Handbook of Computer-Communications Standards Vol. 1、2版、1990で解説されており、ここでも引例として組み込まれている。

【0118】図7は、図6で示したデジタル複写機24の機械的配置を示している。図7において、101はスキヤナ用のファン、102はレーザプリンタで使われる

ポリゴンミラー、103はレーザ（図示せず）からの光線を平行にするのに用いられるF θ レンズを表わしている。

【0119】104はスキャナからの光を検出するためのセンサ（CCDセンサ）、105はスキャナからの光をセンサ104へ集光するレンズ、106は感光ドラム132上の画像を消去するために用いられるケンチング・ランプである。107はコロナ放電器、108は現像ローラーである。109はランプで走査する原稿に光を照射するのに用いられ、110、111、112はミラーであり、光をセンサ104に反射させるために使われる。

【0120】113はドラムミラーで、ポリゴンミラー102からの光を感光ドラム132に反射させるために使われる。114はファンであり、デジタル複写機24の充電領域を冷却するために使われ、115は第1給紙ローラーで、第1給紙カセット117から用紙を給紙するために使われ、116は手動送りテーブルである。同様に、118は第2給紙カセット119のための第2給紙ローラーである。

【0121】120はリレー・ローラーを示し、121はレジストローラー、122は画像濃度センサ、123は転写／分離コロナ放電器をそれぞれ示している。124はクリーニング装置、125は真空ファン、126は搬送ベルトを示し、127は圧縮ローラー、128は出口ローラーを示している。129はホット・ローラーであり、トナーを用紙に定着させるためのものであり、130は排気ファン、131はメイン・モータでデジタル複写機の駆動に使われる。

【0122】図8は、図7で示したデジタル複写機24の電子部品のブロック構成図である。CPU160はマイクロプロセッサで、システム・コントローラとして作動する。162はRAM（ランダム・アクセス・メモリ）であって、デジタル複写機のパラメータの操作を含む、ダイナミックに変化する情報を保存する。

【0123】ROM（読み出し専用メモリ）164はデジタル複写機を運転するために用いられるプログラム・コードと、その複写機を示す、例えばモデル番号（装置番号）やシリアル番号等の情報を保存する。

【0124】166はマルチ・ポート通信インターフェース（I/F）で、デジタル複写機が外部装置と通信できるようにするためのものである。168は電話またはISDN回線を示し、170はネットワークを示している。さらに、マルチ・ポート通信インターフェースに関する情報は図9で説明されている。

【0125】I/F（インターフェイス）コントローラ172は、操作パネル174をシステム・バス186に接続するために用いられる。この操作パネル174には、例えば、コピー枚数、縮小／拡大、濃度調整等の複写機の操作を行うためのコピー・ボタンやキー等を有す

るデジタル複写機で通常見られる入出力装置が装備されている。さらに、液晶表示装置が操作パネル174に組み込まれており、デジタル複写機のパラメータやメッセージをユーザーに表示する。

【0126】記憶部インターフェース（I/F）176は、各種記憶装置をシステム・バス186に接続する。これらの記憶装置には従来のEEPROMであるフラッシュメモリ178やディスク182が含まれている。このディスク182にはハード・ディスク、光ディスクおよび／またはフロッピー・ディスク・ドライブが含まれる。記憶部インターフェース176に接続された接続部180で、追加のメモリ装置をデジタル複写機に接続させることが可能である。

【0127】フラッシュメモリ178は、まれにではあるが複写機の寿命を変化させるデジタル複写機のパラメータを示すための半固定データを保存するために用いられる。このようなパラメータにはデジタル複写機のオプションや構成が含まれている。オプションインターフェース（I/F）184によって、外部インターフェース等の追加のハードウェアがデジタル複写機に接続可能となる。

【0128】図8の左側にはデジタル複写機を構成している各部が図示されている。202はソータを表わし、デジタル複写機の出力をソートするセンサとアクチュエータを有している。200はデュプレクサ（duplexer）であって、複写操作をデジタル複写機によって実行させる従来のセンサやアクチュエータを備えている。

【0129】このデジタル複写機は大容量トレイユニット198を有し、それによって多数の用紙を保持する用紙トレイがデジタル複写機で使用可能となる。大容量トレイユニット198には従来のセンサとアクチュエータが備えられている。

【0130】用紙送りコントローラ196は、デジタル複写機へ用紙を補給したり、通過させたりする制御を行うために用いられる。スキャナ194は、画像をデジタル複写機へ取り込むために用いられ、また、光やミラー等の従来のスキャン用構成要素を有している。

【0131】さらにスキャナセンサがホーム・ポジション・センサとして使用されることにより、スキャナがホーム・ポジションにいることを判断し、またランプ・サーミスタとして使用されることにより走査ランプの正常な操作を確認する。192はプリンタ／イメージャであって、デジタル複写機の出力をプリントし、従来のレーザ・プリント機構や、トナー・センサーや、画像濃度センサ等を備えている。

【0132】定着装置（フューザ）190は高温ローラーを使ってトナーを用紙に熔融定着させるために用いられ、出口センサや、フューザのオーバーヒートを防ぐサーミスタや、オイルセンサを備えている。また、188

はオプション用ユニットインターフェース(I/F)であって、デジタル複写機に追加することができる、例えば自動原稿送り装置、異なるタイプのソータ/コレクタ、あるいはその他の構成要素等の、オプションとしての構成要素に接続するために用いられる。

【0133】図9は、マルチ・ポート通信インターフェース166の細部を図示したものである。デジタル複写機は以下のようなインターフェースを介して外部装置と通信することが可能である、つまり、プリントされる情報の受信、送信を行うセントロニクスインターフェース(I/F)220、SCSIインターフェース(I/F)222、電話回線168Aに接続する従来の電話インターフェース(I/F)224、ISDN回線168Bに接続するISDNインターフェース(I/F)226、RS-232インターフェース(I/F)228、そしてLAN170に接続するLANインターフェース(I/F)230等である。

【0134】一つでローカル・エリア・ネットワークと電話回線の両方に接続する装置がMegahertz社から市販されており、イーサネット・モデム(Ethernet-Modem)として知られている。

【0135】CPUや他のマイクロプロセッサ、あるいは集積回路は、デジタル複写機に実装された各センサの状態をモニターするためにモニター処理を行い、一連の処理はデジタル複写機の制御と操作に用いられるコードの指令を実行するために行われる。さらに、デジタル複写機の全体的操作を制御するために中央システム制御処理が行われ、デジタル複写機に接続された外部装置との通信を確実に行うために通信処理が行われる。

【0136】システム制御処理は、図8のROM164のようなスタティックメモリや、フラッシュメモリ178やディスク182のような半スタティックメモリ等に保存されたデータや、あるいは、RAM162やフラッシュメモリ、あるいはディスク182のような揮発性または不揮発性メモリ等に保存されているダイナミックデータ等をモニターし、コントロールする。さらにはスタティックデータはROM164以外の装置、例えばフラッシュメモリ178かディスク182のどちらかを装備した不揮発性メモリに保存することが可能である。

【0137】前述した詳細な説明は被モニター装置としてデジタル複写機に関して述べたものであるが、本発明の被モニター装置としては、複写機以外のビジネスオフィス機器、例えばファクシミリ装置、スキャナ、プリンタ、ファクシミリ・サーバ、あるいは上記以外のビジネスオフィス機器等に同様に適用できる。

【0138】さらに、本発明には、例えば、ガスや水等の計量システム、あるいは電気計量システム、自動販売機、あるいは機械操作を行う上記以外の装置のように、通信用の接続通信モードあるいは無接続通信モードを用いることにより操作し、しかもモニターを必要とし、ま

たその機能を行う上記ビジネス装置以外の装置類も含まれる。特殊な装置やコンピュータをモニターすることに加えて、本発明は、汎用コンピュータのモニター、制御、診断にも用いることが可能である。

【0139】図10は、診断、モニター、制御用装置によってビジネスオフィス機器等の新しい装置を正確に認識させるために行われるプロセスを含んだフローチャートを示している。スタートすると、ステップ250でユーザーやモニター装置はビジネスオフィス機器(被モニター装置)に名前やアドレスを割り当てる。通信を送受信する装置にとっては、通信の送り先や通信の送信元を知る必要がある。

【0140】ステップ252では、図8で図示したフラッシュメモリ178やディスク182等の半スタティックメモリにその名前やアドレスを保存する。この情報は、電話回線やISDN回線を通じて行う接続通信モードと、従来のインターネット・電子メール手順を用いるような無接続通信モードとの両方に用いられ、また同様に、通常はローカル・エリア・ネットワークを介して印刷を行うためにデジタル複写機を使用しているような装置と通信を行うためにも用いられる。

【0141】ビジネスオフィス機器に関する情報が一度決定され、その情報がステップ252で保存されると、他の装置から上記ビジネスオフィス機器にアクセスできるようにこの情報を登録しなければならない。したがって、ステップ254で、この装置の名前とアドレスは、例えば、接続しているネットワークで電子メールを送受信するメール・サーバに登録される。

【0142】またローカル・エリア・ネットワークの一部としてビジネスオフィス機器を登録することも望ましい。さらに、ビジネスオフィス機器がメッセージを送信するモニター装置類もビジネスオフィス機器と共に登録される。最終的には、このビジネスオフィス機器は、顧客サービス部門のコンピュータや、あるいはリモート装置(モニター装置)がビジネスオフィス機器を正確にモニターし、ビジネスオフィス機器の状態を把握するためのリモート・モニタリング、制御および/または診断用コンピュータ(例えば、ワークステーション)と共に登録される。

【0143】ステップ256では、名前、アドレス、モデル番号、シリアル番号、あるいはこれら以外の、顧客サービス用の装置の特性、あるいは異なるタイプのデータベースを登録するために、図6で図示したサービス部門やその他の部門へメッセージを送る。

【0144】図11は ビジネスオフィス機器のような装置への通信元を判断するためのフローチャートを示している。スタートすると、ステップ260でその入力かシステム操作用のものか、あるいは診断、モニタリング、リモート・コントロール操作用のものかを判断する。

【0145】ステップ260においてその入力システム用のものであると判断されると、ステップ262で、通常のシステム入力処理のための入力チャンネルが設定される。例えば、その装置がプリンタの場合は、受信情報は印刷を行うために用いられる。

【0146】一方、ステップ260においてその入力システム用ではなく、装置のコントロール、モニタリング、あるいは診断用であると判断されれば、ステップ264でその入力に適切なアプリケーションが捜される。代表的なアプリケーションは装置のモニタリングまたはテストのためのプロセスであろう。

【0147】ステップ266では捜しているアプリケーションが見つかったかどうかを確認し、もしまだであれば、エラーが表示され、処理が終了する。そうでない場合は、ステップ268でアプリケーション入力処理のための入力チャンネルが設定され、システムは入力情報の処理が可能となる。

【0148】図12は、デジタル複写機等のビジネスオフィス機器への入力メッセージあるいは該ビジネスオフィス機器からの出力メッセージを処理するデータ・フロー図を示す。直接接続プロセス270は、ローカル・エリア・ネットワーク、電話回線、あるいはISDN回線を通じて行うような接続通信モードの入力通信および出力通信を処理するために用いられる。入力メッセージはバッファ274を通過して、公知の従来の方法で入力情報をパージングするパージング・プロセス292へ達する。

【0149】この入力情報によって、294、296、298で図示されているアクション等多数のアクションが行われる。アクションの中にはメッセージの送り戻しを要求するものがあり、その戻されるメッセージはバッファ300へ向けた矢印によって図示されている。次に、出力メッセージ・プロセス302が実行され、直接接続が無接続プロセスのいずれかに向けて出力メッセージを用意する。直接接続プロセスは直接接続プロセス270を通過する前にバッファ272を通過する。

【0150】無接続通信モードには無接続入力プロセッサ276と無接続出力プロセッサ278がある。無接続入力通信はバッファ280を通過し、ステップ284で解読プロセスは実行される。解読された情報はバッファ286に保存され、従来のパージング・プロセス292に送られる。

【0151】上記で説明したように、アクション294、296、298の内、一つ以上のアクションが実行され、出力メッセージがバッファ300を通過して出力メッセージ・プロセス302に入る。その後、無接続通信モードの出力メッセージはバッファ290を通り、暗号化プロセス288によって暗号化される。暗号化されたメッセージはその後バッファ282を通り、無接続出力プロセッサ278を介して終着点であるインターネット

等の無接続ネットワークに送信される。

【0152】無接続通信モードであればいずれのタイプでも、本発明により使用することが可能である。無接続メッセージを送る安価で利用可能な媒体はインターネット電子メール・メッセージである。無接続入出力プロセスは、SunOS(4.1.X)に装備されているBSD Unixメール・システムで使用されるような、公知のインターネット・Eメール・プロトコル等によるものでもよい。

【0153】また、インターネット・Eメールの操作について説明している他の情報も、当のインターネット上でいろいろなソースを通して利用可能である。インターネットは無接続通信モードとして安価な方法ではあるが、一方で、インターネット電子メール・システムはスピードが遅く、また信頼度も低く、したがって、状況によっては無接続プロセスを利用する代わりに以下に述べるような直接接続が行われる。

【0154】図13は、図12で図示されたデータ・フロー図を実行するために用いることができるフローチャートを示す。スタートして、まずステップ340で解読が必要であるか否かが判断されて、解読が必要であれば、ステップ342で解読ルーチンが実行される。その後ステップ344で、従来の方法によりパージングを行うパーサを呼び出し、アクションが採られるべきかどうかをステップ346で判断する。

【0155】もし必要であれば、例えば、情報がリモート・モニター、診断あるいは制御装置に送り返されるものである場合は、ステップ348で必要なルーチンが呼び出される。ステップ350では、それ以上の処理が必要で、フローがステップ340に戻りさらに処理を行うかどうかを判断する。それ以外はフローは呼び出しプロセスに戻る。

【0156】図14は、接続通信モードと無接続通信モードのいずれが必要か装置が判断する過程で行われるプロセスを図示したものである。スタートすると、ステップ370でイベント通信が必要かどうか判断され、もし必要なければフローは呼び出しプロセスに戻る。もし通信が必要であれば、ステップ372でそのイベントが接続通信モードと無接続通信モードのいずれを必要としているか判断する。急送順位に基いて、緊急の対処を必要とする最優先イベントか、あるいはリモート・モニター装置が関心を持つ最優先イベントのいずれかが接続通信モードに送られる。

【0157】上記イベントは装置内の接続が危険である場合や、装置内の何かが緊急な対処を必要としている場合等に用いられる。例えば、定着ユニット内のサーミスタが高温で危険を感知した場合は、直接接続通信モードが用いられる。しかしながら、装置の使用状況や正常な状態を示す週単位あるいは月単位のレポートの送信にはより遅い無接続通信モードを使用することができる。さ

らに、無接続通信モードが正常に機能しない場合には、接続通信モードが用いられる。

【0158】例えば、インターネット・電子メール・メッセージがモニター装置で正常に受信されない場合は、直接接続通信モードが用いられる。Eメール・メッセージには受信通知を送ってくれるよう要請してあるが、その通知が一定の時間（例えば3～24時間）を過ぎても届かない場合には、そのメッセージを再度送信するために接続通信モードが利用される。また、接続通信モードが正常に機能しない場合には、無接続通信モードが利用される。

【0159】ステップ372でイベントが無接続通信モードを必要としないと判断されると、ステップ376で直接接続チャンネルを用意するかどうかを判断する。例えば、電話回線かISDN回線が利用できるかどうか判断する。もしできる場合は、直接接続プロセスがステップ378で行われ、適切な情報が送信される。

【0160】もし直接接続チャンネルが利用できない場合は、ステップ380で操作パネルを通してユーザーに対し、電話、ISDN、あるいはそれ以外の直接接続装置、あるいは通信装置に問題があることを知らせる。ステップ372でそのイベントが無接続通信モードを必要としていると判断した場合は、ステップ374で無接続通信プロセスが呼び出され、図14のプロセスは呼び出しプロセスに戻る。

【0161】図15は、遠隔的に診断、制御される被モニター装置によって開始する無接続通信モードを図示したものである。まず最初に、被モニター装置がその識別情報をステップ390で送信する。被モニター装置はステップ394でデジタル複写機の濃度情報の分析を要請する。モニター装置は、デジタル複写機の印刷濃度が濃すぎるか薄すぎるかを判断するために、送信された識別情報に対応する特定のデジタル複写機の濃度情報を分析する。

【0162】ステップ396で濃度分析の結果が被モニター装置に送り返される。図15のプロセスが接続通信モードを利用していれば、モニター装置は、識別情報の受信を通知するステップ392を実行し、またステップ394はその通知が届くまでは実行されない。しかし、無接続通信モードにおいては、ステップ392は行われず、識別情報の送信が行われると直ちにその分析の要請を行う。

【0163】被モニター装置がビジネスオフィス機器として使用されているので、これらの機器を制御、診断、モニターするリモート装置（モニター装置）は、接続通信モードか無接続通信モードのどちらかを初期設定することができる。

【0164】上記のように使用される装置（システム）であるので、リモート・モニター装置が緊急情報を送る必要ができた場合、あるいはその装置（機器）から緊急

の応答を必要とする場合は、接続通信モードが用いられる。緊急を要しない場合は、リモート装置は無接続通信モードを利用する。

【0165】例えば、ビジネスオフィス機器に危険な状況をもたらすプログラム内のバグのために、新しい制御用ソフトウェアをビジネスオフィス機器にダウンロードする必要ができた場合は、直接接続通信モードが用いられる。また、被モニター装置について説明したように、もしモニター装置が通信用の上記モードの一つに問題を発見すると、別のモードが用いられる。

【0166】図16は、モニター装置によって初期設定された接続通信モードを図示したものである。まず最初に、ステップ400で、被モニター装置の識別情報が要請され、ステップ402で被モニター装置はその識別情報を送信する。ステップ404では、モニター装置は送信された識別情報を照合し、データベースの中で識別された装置の特性を調査する。データベースによって被モニター装置あるいは機械の、例えば、整備状況や、オプション装置、使用情報、あるいは上記以外の情報等の各種情報が得られる。

【0167】ステップ406でモニター装置は被モニター装置に画像濃度情報を要求する。ステップ408では、被モニター装置は画像濃度情報の要求を受けて、画像濃度情報を判断し（または以前に保存していた画像濃度情報を調べて）、ステップ408でモニター装置へその画像濃度情報を送信する。ステップ410では、モニター装置は受信した情報を分析し（つまり受信した情報とデータベースで調べた情報とを比較し）、被モニター装置のパラメータの変更が適切であると判断する。

【0168】ステップ412では上記装置のパラメータ変更を要請し、適切なコマンドが送られる。ステップ414では被モニター装置が受信したコマンドに応じて操作パラメータを変更される。

【0169】図17(a)～図17(c)は、本発明で使用される各種データベースの構成を表わしている。図17(a)のデータベース構成440は、装置ID442、装置番号444、シリアル番号446、コマンド・レベル448、およびアドレス450を有する簡潔なデータベースを表わしている。装置ID442は装置自体を表わす唯一のもので、図17(b)～図17(c)に表わされるデータベース等、装置を説明する様々なデータベースをリンクさせるために用いられる。

【0170】コマンド・レベル448は装置が複雑な指令セットを処理することができるかどうかを示している。アドレス450は接続と無接続のアドレス情報を有しており、その中にはネットワーク・アドレス、電話番号、名前、その他装置（または機械）を識別するための必要な情報が含まれている。

【0171】図17(a)のデータベースには、図17(b)と図17(c)のデータベースがリンクし、各デ

ータベースにはそれぞれ付属装置の情報や装置の履歴等が記されている。図 17 (b) に図示されているデータベース構成 460 は図 17 (a) のデータベースに入っている装置の付属装置やオプションのためのものであり、また図 17 (a) の装置 1D442 に対応する装置 1D462 を有している。

【0172】 付属装置 1D464 はソータ、自動用紙送り装置、これら以外の付属装置等、装置に接続される選択的な付属装置のタイプを示している。付属装置シリアル番号 446 は装置に接続される付属装置のシリアル番号である。付属装置 1D464 は付属装置データベースの様々な特徴を記したデータベースにリンクすることができる。他のデータは付属装置およびオプションのデータベース 460 に含まれている。

【0173】 装置の履歴については、図 17 (c) に表わされている別個のデータベースに保存されている。データベースの構成 470 には様々なデータベースとリンクするために用いられる装置 1D472 が同様に含まれている。日付と時間 474、それに情報 476 は、誤作動や特殊な状況、および事象が発生した日付と時間を含む装置内の事象を記すために用いられる。

【0174】 図 17 (a) ~ 図 17 (c) に図示されたデータベースは、装置に関して保存された情報のタイプを示している。別個のデータベースとして示されてはいるが、それらのデータベースを実現するということは多かれ少なかれ種々のデータベースを含む可能性を持っている。会社の中の異なる部門は各装置に関する情報を記したそれぞれ独自のデータベースを持っている。

【0175】 整備データベースには個々の装置に関する一番完全なデータベースが入っており、各装置の完全な整備歴が含まれており、顧客サービス部門で保存してもよいものであろう。製造、エンジニアリング、マーケテ

ィング部門のデータベースもそれぞれ維持することが可能となり、装置から発生する情報を利用することができる。異なるデータベースは異なる分野を通じてリンク可能となる。

【0176】 例えば、サービス・データベースは装置のシリアル番号とモデル番号を通じて製造データベースとリンク可能となる。製造データベースとエンジニアリング・データベースとはバージョンとモデル番号とを通じてリンク可能となり、またサービス・データベースとエンジニアリング・データベースとはモデル番号を通じてリンク可能となる。公知のデータベース・システムは情報を維持し、必要に応じてそれを共有するために利用される。

【0177】 分析/決定ソフトウェアが別個に作成されてもよく、それによってユーザーが一つあるいはそれ以上のデータベースに対して特定の照会をすることが可能となる。ユーザーは、知りたい情報を作成するためにどのようなタイプの質問でも、また検索されるデータベースはどのようなものでも明確に提示できる。分析/決定ソフトウェアは装置に関する情報を記す月毎かあるいは定期的なレポートの作成用にも用いられ、また誤作動が起きた場合の警告やその他の注意を発生させることができる。

【0178】 表 2 ~ 表 4 は、デジタル複写機、プリンタ、ファクシミリ装置用に作成された 1 月間の報告メッセージを示している。これらの報告はパラメータ、利用状況、それ以外の装置の情報を簡単に示しているが、もちろん、必要に応じて情報を入れ替えても、新たに付け加えてもよい。

【0179】

【表 2】

デジタル複写機： 月間報告メッセージ	
-	コピー枚数と作業回数
-	変更部分検索リスト
-	変更パラメータ・リスト
-	二重伝送の利用
-	縮小の利用
-	拡大の利用
-	各種用紙サイズのコピー枚数
-	手動送りの利用

【0180】

【表 3】

プリンタ： 月間報告メッセージ	
-	コピー枚数と作業回数
-	変更部分/供給リスト
-	設定変更リスト
-	二重伝送の利用 (可能な場合)
-	各種用紙サイズのコピー枚数
-	各種プリンタ言語：PCL5, ポストスクリプト毎の作業回数
-	手動送りの利用

【0181】

【表 4】

ファクシミリ装置： 月間報告メッセージ	
-	送信と受信回数
-	送信ページ枚数
-	受信ページ枚数
-	スピード・ダイヤル等の特殊性能利用回数

【0182】表5は、ここで説明される通信操作を実現するために用いられる種々の通信用コマンドを表わしたものである。表の左側にはオペレータがあり、右側にはオペランドがある。この表ではTは特定のアドレス、パラメータ、センサ、あるいは保存されたデータである対象を表わし、Vは数値を表わす。

【0183】表5に示されたセット・コマンド(Set)は、所定のアドレス、パラメータ、あるいは保存されたデータをVに入れられた数値に設定する設定コマンドである。同様にゲット・コマンド(Get)はそれによって所定の対象情報を得ることができる。報告オペレータはゲット・オペレータによって要請された情報に関する被モニター装置からの報告に含まれる。"set __li

st、get__list、およびreport__list"はこれらのコマンドによって、一つのオペレータを用いるだけで一つ以上の対象と数値を得ることができ、また設定し、作成することが可能である。

【0184】表のコピー・コマンドによって、情報が一つのメモリ・アドレスから別のメモリ・アドレスへ、またメモリ・アドレスからディスクへ、ディスクからメモリ位置へコピーされる。"command __not __understood operator"は所定のオペレータおよび/またはオペランド(または複数の)が理解できなかったことを示している。

【0185】

【表5】

オペレータ	通信用コマンド オペランド	T: 対象, V: 数値
Set	T V	
Get	T	
Report	T V	
Set_List	T1 V1, T2 V2, . . . , Tn Vn	
Get_List	T1 T2, . . . , Tn	
Report_List	T1 V1, T2 V2, . . . , Tn Vn	
Copy_Memory_To_Memory	コピー元 コピー先 Num_Byte	
Copy_Memory_To_Disk	コピー元 名前 Num_Byte	
Copy_Disk_To_Memory	名前 コピー先	
Command_Not_Understood	オペレータとオペランド	

【0186】表6はリモート・モニタリング・診断装置(モニター装置)から複写機へ送られるコマンドを表わし、表7は表6のコマンドを受信した後の複写機からの応答を表わしている。表6の"get id"コマンドを出した後の、複写機からの応答は"id"が"AX301B3330"となっている。表7の2行目は"list"の使用を表わしている。この場合、上記構成は一つ以上の対象パラメータを含んでおり、したがって、対象パラメータのグループとその数値とは"LIST"オペレータの後に来る。

【0187】表6と表7の情報は表示目的で作成されたものである。複写機を起動させるための第2と第3のコマンドに含まれるソータと自動原稿送り(adf)を設

定することにより、複写機からの応答は発生しない。ゲット構成コマンドに回答して、複写機からの第2の応答で、報告が複写機から作成される。

【0188】また、所定のメモリ位置A100のゲットと設定が表6と表7に表示されている。表6の最後のコマンドは立ち上げをA100に設定することである。この設定は複写機の再立ち上げ、あるいは再初期化の時点で、メモリ位置A100が読みとられることを意味している。

【0189】

【表6】

複写機へのコマンド		
get	id:	
set	sorter	yes:
set	adf	yes:
get	configuration	:
get	A100 :	
set	A100	FFAA :
get	copy_count	:
get	jam_count	:
get	last_toner_change	:
set	boot A100	

【0190】

【表7】

複写機からの応答		
report	id	AX301B3330
report	configuration LIST (sorter yes, adf yes, large_capacity_tray no.....) :	
report	A100 AABB :	
report	A100 FFAA :	
report	copy_count	9895 :
report	jam_count	0 :
report	last_toner_change	12Apr95 :

【0191】装置がLANを介してインターネットとアクセスすることに加えて、インターネット・アクセス・プロバイダや、America On Lineのようなダイアルアップ・サービスを介して、電話回線やISDN回線を通じてインターネットにアクセスすることも選択的に可能である。この方法によれば、ネットワークと接続していない装置でもまた無接続通信モードを利用することができる。この場合、装置は受信したインターネット・Eメール・メッセージを受け取るために定期的にインターネット・プロバイダにダイヤルしなければならない。

【0192】一つのビジネスオフィス機器あるいはその他の機械に関する診断および統計的情報は秘密、あるいは固有情報とみなすことができ、従って、人々はそうした情報が不特定多数によって見られることを望まない場合がある。送信されたデータを無許可で見られるのは、情報がインターネットで送られる場合、特に懸念される。

【0193】さらに、リモート・モードでモニターされるべきではない機械あるいはビジネスオフィス機器からの情報などのような秘密情報や、あるいは一つのビジネスオフィス機器の診断およびステータス情報のように偽装されていてインターネット上でそのビジネスオフィス機器と関係づけられない情報が送信されるのを防ぐのが望ましい。

【0194】図18および図19のフローチャートは例えば一つの会社からインターネットを通じて離れた場所にあるデータ・センターに送られた情報をモニターするためのプロセスを示している。

【0195】同ネットワークを通じて送られる情報は、プリンタ32、ファクシミリ装置28、デジタル複写機

／プリンタ24、その他のいずれかのタイプの機械、あるいはネットワーク17に接続されたワークステーションのいずれか一つなど、図6でネットワーク17に接続された装置のいずれか一つから発信される。送信される情報は好ましくは装置の機械的ステータスなどの状態を検出して、検出された状態を電氣的に出力する電気機械式センサーから発信される。

【0196】この電気機械式センサーはいずれの可動部分を持たないように構成することもできるし、例えば、紙の存在を検出する光学センサーとして実現することもできるが、その電気機械式センサーはビジネスオフィス機器のいずれかの他の特徴を検出してもよいし、いずれの望ましい形態で実施しても差し支えない。

【0197】情報は、例えば、防護装置14を介して、インターネット10を通じて、電子メールとして送られたり、防護装置40を介してワークステーション42などのビジネスオフィス機器のデータを処理し、モニターするデータ・センターに送られたり、あるいは防護装置50を介してネットワーク52に接続されたワークステーションのいずれかに送られる。ネットワーク17からの発信メッセージをモニターするセキュリティ・センターはネットワーク17に接続されたいずれかのワークステーションにおいて実施されるか、あるいは防護機構14の内部において実施される。

【0198】図18に示されるプロセスにおいては、スタート後、ステップ502でビジネスオフィス機器32、28あるいは24の一つなどの機械によってステップ502で送信されるメッセージが構成される。このメッセージは次にビジネスオフィス機器の一つ、またはそのビジネスオフィス機器に接続された別のメカニズムによってステップ504で暗号化される。

【0199】暗号化されたメッセージは次にステップ506でワークステーション42あるいはネットワーク52に接続されたワークステーションの一つなど受信されたメッセージをモニターし処理するデータ・センターなどの意図された受信先に送られ、また、セキュリティ装置とも呼ばれ、ネットワーク17に接続されたワークステーションの一つを用いて、あるいは上記ファイアウォール14内で実施される場合があるセキュリティ・センターにも送信される。

【0200】セキュリティ・センターとデータ・センターの両方にメッセージを送ることで、そのセキュリティ・センターあるいはセキュリティ・グループが防護装置14を介してインターネットを通じて送られたのと同じメッセージを確実に受信できるようにする。

【0201】別の方式として、メッセージをセキュリティ・センターにおくるビジネスオフィス機器の代わりに、防護装置14が上記セキュリティ・センターを通じてそのメッセージのコピーをセキュリティ・センターに送り、そのセキュリティ・センターがインターネットを通じて送られたメッセージの本物のコピーを確実に受信できるようにしてもよい。

【0202】発信メッセージは好ましくはステップ508で防護装置14に含まれるログあるいはデータベースに保存される。このロギングはそのメッセージのコピーも受信するセキュリティ・センターが（以下に述べるステップ530で）すべての発信メッセージのコピーが受信されていることをチェックできるようにするために行われる。

【0203】そのメッセージが発信された機械をモニター、診断、および／または補修するためにそのメッセージを処理するデータ・センターなどの意図された受信先において、暗号化された情報が受信され、ステップ510で解読されて、ステップ512でその機械をモニター、診断、および／または制御するために処理される。同時に、電子メールなどの暗号化されたメッセージが受信、解読され、そしてステップ520でネットワーク17に接続されたワークステーションの一つなどのセキュリティ・センターか、あるいは防護装置14によって記憶される。

【0204】ステップ522で、セキュリティ・センターは何の情報が送られてきているのかについて判断する。ステップ522を実行するためには、例えば汎用コンピュータ上で実行されるコンピュータ・プログラムを用いて解読されたメッセージを復号化できるようにすることが必要である。

【0205】例えば、ビジネスオフィス機器の一つから送信されるデータは二値形式であるかもしれないし、人間や機械が簡単に処理、あるいは理解することができる他の形式であるかもしれない。従って、そのコンピュータ・プログラムを用いて、送られてきているデータの本

当の意味を判定することが必要である。

【0206】ステップ524で、ステップ504で暗号化されたメッセージ内に含まれている情報を送信することが受け入れ可能、あるいは許可できるかどうかについて判断する。このデータが秘密保持の必要性の高くないビジネスオフィス機器の状態を述べており、従ってリモートでモニターされてもよい標準的なデータであれば、そのデータは送信することができる。

【0207】さらに、ステップ524でそのデータを送信するのが認められないと判断されれば、ステップ526において、セキュリティ装置のヒューマン・モニターに対する警告などの警告が発せられる。

【0208】次に、ステップ528で、必要な場合、そのデータを送信している機械からのさらなる通信を禁止する。そのデータがリモートでモニターされたり制御されたりされてはならない機械からのものであったり、あるいはそのデータが送信されてはならない秘密情報を含んでいるような場合に、そのデータを送信することは認められるべきではない。

【0209】数日間、一週間、あるいは一か月などの最初の期間が経過した後、ステップ524のチェックは送信される一つ一つのメッセージに対して行う必要はないが、発信メッセージをランダムにチェックしてもよい。このランダム・チェックは個人がメッセージをチェックする負担を軽減する。しかしながら、発信メッセージが機械によってチェックされる場合は、すべての発信メッセージをモニターするのが好ましい。

【0210】次に、ステップ530で防護装置14を通過するログに記憶されている機械またはオフィス機器の発信メッセージがセキュリティ・センターに対応するメッセージを持っているかどうかを判定する。セキュリティ・センターが防護装置14とは別の機械として実施されている場合、データ・センターなどの意図された受信先とセキュリティ・センターの両方に暗号化されたメッセージが送られるように常時ステップ506が適切に行われれば、セキュリティ・センターは防護装置のログに保存されている各メッセージに対応するメッセージを受信している筈である。

【0211】しかしながら、誰か、あるいは一つの機械が防護装置14を介して認められていないメッセージを送信しようとする場合、このメッセージのログは保存され、セキュリティ・センターは対応するメッセージを受信しないであろう。ステップ530で防護装置14を介しての発信メッセージとセキュリティ・センターによって受信されたメッセージとの間に対応性がないと判断された場合、ステップ532に進み、警告ランプを点灯したり、可聴警告を発生したり、あるいはコンピュータ・メッセージを発生したりしてセキュリティ装置のヒューマン・モニターに警告を出す。

【0212】すると、ステップ534で、必要な場合、

データを送信している機械からのさらなる通信が禁止され、防護装置を介してのすべての通信が禁止され、あるいは別のタイプのセキュリティ動作が実行される。そして、図 18 に示されているプロセスが終了する。また、ステップ 530 で防護装置 14 を通過するログされたすべてのメッセージがセキュリティ・センターに対応する記録 (entry) を有していると判断されると、そのプロセスが終了する。

【0213】図 18 に示されているステップに代わるものとして、ステップ 506 で暗号化されたメッセージを意図された受信先とセキュリティ・センターに同時に送る代わりに、メッセージを先ずセキュリティ・センターに送り、意図された受信先への送信は、その情報をステップ 524 および 530 で送信することが受け入れられると判断されるまで遅らせる。

【0214】さらに別の方式として、ステップ 524 で発信した装置および／または受信先装置の電子メール・アドレスをモニターする。これらのアドレスの一つまたは両方がデータベース内に保存されている許可可能なアドレスのリストに合致しない場合、警告が出され、さらなる通信が禁止され、そして／または試みられた不適切な伝送の発生を信号伝送するための他の行為が実行される。

【0215】図 19 は発信伝送をモニタリングするための第二の実施の形態を示している。スタート後、ステップ 552 でプリンタ 32、ファクシミリ装置 28、デジタル複写機・プリンタ 24、あるいはそれに接続された装置によって送信されるメッセージが構成される。

【0216】このメッセージはステップ 554 で、ネットワーク 17 に接続されたワークステーションのいずれか、あるいは防護装置 14 内で実施されているセキュリティ・センターに暗号化されていない形式で送られる。ステップ 554 で暗号化されていないメッセージをセキュリティ・センターに送ることによって、セキュリティ・センターは、以下に述べられるように、防護装置を介してインターネットを通じてデータ・モニタリング・センターに送られるメッセージと比較される。

【0217】さらに、その後、ステップ 556 で、ビジネスオフィス機器などの機械か、あるいはそのビジネスオフィス機器に接続された別の装置によって、送信されるべきメッセージが暗号化される。この暗号化されたメッセージは次にステップ 558 で防護装置 14 に送られる。ステップ 560 で、防護装置 14 はそのメッセージをインターネットを介して意図された受信先に送り、また、その暗号化されたメッセージのコピーを上記セキュリティ・センターに送り返す。

【0218】そして、ステップ 561 において、防護装置 14 で送られたメッセージがセキュリティ・センターで解読化される。次に、ステップ 562 でステップ 554 で防護装置 14 から受信されたメッセージを防護装置

14 から受信されたメッセージと比較する。それらのメッセージが同じでないと判定された場合に、人オペレータに対する警告などの警告がステップ 564 で出され、必要であればさらなる通信が禁止され、あるいはステップ 566 で他のセキュリティ動作および予防措置が取られる。

【0219】そうすると、図 19 のプロセスが終了する。ステップ 562 でビジネス機器からのメッセージが防護装置で受信されたメッセージと同じでないと判定された場合、図 19 のプロセスは終了する。

【0220】また、図 19 のプロセスが終了する前に、例えば、ステップ 562 が肯定的な結果に終わるか、あるいはステップ 566 の後で、発信されたメッセージの内容をチェックするステップを図 18 のステップ 524、526、および 528 が実行されるのと同じ方法で実行することができる。

【0221】暗号化されたメッセージを防護装置を介してインターネットを通じて送り、同時にセキュリティ・センターにその暗号化されたメッセージのコピーを送るのに代えて、ステップ 562 でセキュリティ・センターがそのビジネスオフィス機器からのメッセージが防護装置からコピーされたメッセージと同じであると判断するまで、その暗号化されたメッセージを防護装置に保持することもできる。これにより、認められていない通信が防護装置を介してチェック前に送られることを防ぐことができる。

【0222】この発明のセキュリティ面の別の特徴が図 18 および図 19 に示されている。本発明は図 18 および図 19 のそれぞれからの特徴の種々の組み合わせを有する実施の形態を含んでいる。

【0223】図 18 および図 19 のフローチャートに示されているセキュリティ・センターは、そうしたセキュリティがバイパスされたり、不適切に実施されたり、あるいは秘密データが認められていない人によって見られないようにするためにするために、認められた人へのみその使用が認められるようにするべきである。

【0224】上に開示した実施の形態で、最終的に送信されるメッセージはセキュリティ・センターによって中継されるか、あるいは別の方式として、セキュリティ・センターがそのデータのコピーを受信して、そのメッセージ内のデータをビジネスオフィス機器が送信するようにしてもよい。

【0225】本発明においてはまた、セキュリティ・グループが、例えば、過去において秘密漏洩が起きたかどうか、あるいはビジネスオフィス機器の操作の履歴をモニターするために必要になった場合に備えて、発信されるメッセージを記憶、保存することも可能である。

【0226】この発明は、従来の汎用デジタル・コンピュータ・プログラムを、本発明の教示に従って使用することにより従来通りに実行することが可能であり、コン

ピュータ技術に関わる当業者にとっては自明のことである。適切なソフトウェアの符号化は熟練したプログラマであれば本開示の教示に基いて容易に作成し得るものであり、ソフトウェア技術に関わる当業者にとっては自明のことである。

【0227】本発明はまた、アプリケーション用の所定の集積回路を作成することにより、あるいは従来の部品回路の適切なネットワークを相互に接続することにより実行可能となり、当業者にとっては容易に想定し得ることである。

【0228】本発明はまた、記憶媒体としてのコンピュータ・プログラム製品も含み、その中には本発明のプロセスを行うためのコンピュータ・プログラム用インストラクションも含まれる。上記記憶媒体には、フロッピー・ディスク、光ディスク、CD-ROM、光磁気ディスク、ROM、RAM、EPROM、EEPROM、磁気または光カード、あるいは電子的なインストラクションを記憶させるために適した媒体等、あらゆるタイプのディスクが含まれるが、それだけに限定されるものではない。

【0229】上記システムは、本発明の教示に基いて構成された装置や装置に内蔵されたもの、装置の外部に取り付けたもの等の追加型装置を使用する従来のビジネスオフィス機器を含む従来の装置によって使うことができる。

【0230】本発明の改造・変更が上記の教示により多数可能となることは明らかである。したがって、従属の請求項の範囲内であれば、ここで特に説明されたものの以外でも本発明を実施することは可能である。

【0231】

【発明の効果】以上説明したように、本発明に係る通信処理方法および通信処理システムにあっては、被モニター装置とモニター装置（リモート診断装置）との間の無接続通信を可能にすることができる。また、発信無接続通信が確実に承認され、かつその秘密を保持することができる。

【図面の簡単な説明】

【図1】本発明を適用することができる機能システムの全体を示す図である。

【図2】本発明の一実施の形態に係るハードウェア全体構成を示す図である。

【図3】本発明との通信に使用できる符号化スキーマを示す図である。

【図4】パワーオン後の複写機と操作パネル間の通信の一実施の形態を示す図である。

【図5】本発明による診断ステーションの接続方の一実施の形態を示す図である。

【図6】3つのビジネスオフィス機器を、インターネッ

トを介してコンピュータおよびデータベースから成るネットワークに接続した例を示す説明図である。

【図7】デジタル複写機の構成を示す説明図である。

【図8】図7に示すデジタル複写機の電子部品を示す説明図である。

【図9】図8のマルチ・ポート通信インターフェイスの詳細を示す説明図である。

【図10】装置が最初に設置された場合に行われるプロセスを示すフローチャートである。

【図11】装置に入ってくる通信が通常の動作を要求しているのか、それともリモート・モニタリング、診断、および制御のためのものなのかを判断するためのプロセスを示すフローチャートである。

【図12】装置との通信におけるデータ・フロー図である。

【図13】図12のデータ・フロー図のプロセスを示すフローチャートである。

【図14】その装置によって通信が開始された場合に行われる処理を示すフローチャートである。

【図15】被モニター装置からリモート・モニター装置への無接続通信を示す説明図である。

【図16】モニター装置と被モニター装置との間の接続通信モードでの通信を示す説明図である。

【図17】同図（a）はサービス・データベースの主要構成部品を示し、同図（b）は取り付けおよびオプション・データベースの情報を示し、同図（c）は種々の装置の経時データを保存するためのデータベースを示す説明図である。

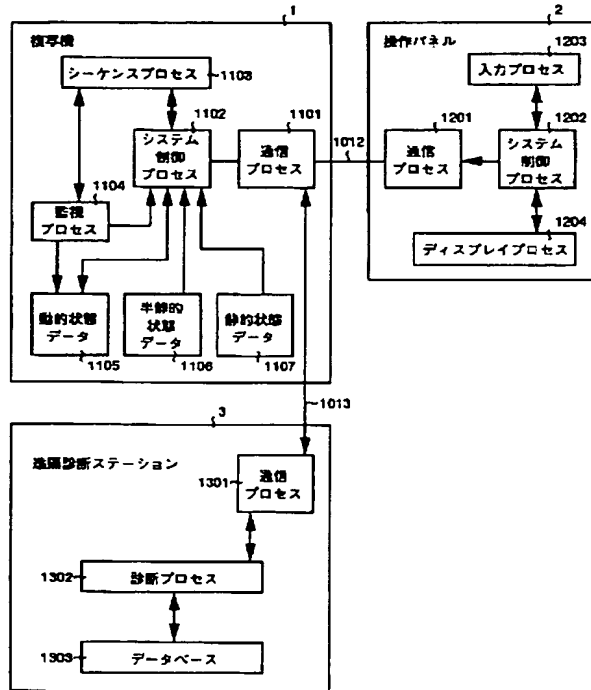
【図18】セキュリティ・センターによるビジネスオフィス機器からデータ・センターへの発信メッセージのモニタリングの第一の実施の形態を示すフローチャートである。

【図19】セキュリティ・センターによるビジネスオフィス機器からデータ・センターへの発信メッセージのモニタリングの第二の実施の形態を示すフローチャートである。

【符号の説明】

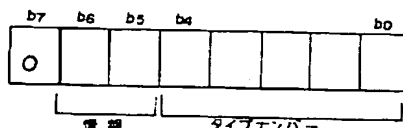
10 インターネット
12A~12I 相互接続コンピュータ
14, 40, 50 防護装置 (fire wall)
16, 18, 20, 22, 56, 62, 68, 74
ワークステーション
17 ネットワーク
24 デジタル複写機 (被モニター装置)
28 ファクシミリ装置 (被モニター装置)
32 プリンタ (被モニター装置)
26, 30, 34 電話回線またはISDN回線
46, 54, 58, 64, 70, 76 ディスク

【図 1】



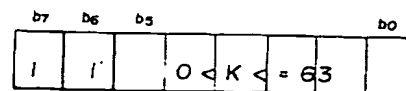
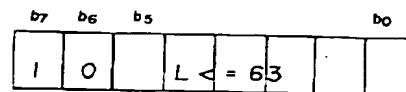
【図 3】

(a) タイプ



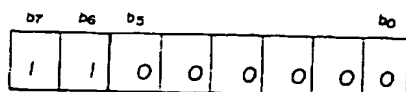
00 正常 1-30 タイプ
 01 エラー
 10 複合
 11 緊急

(b) 長さ



次のKバイトは長さを特定する。

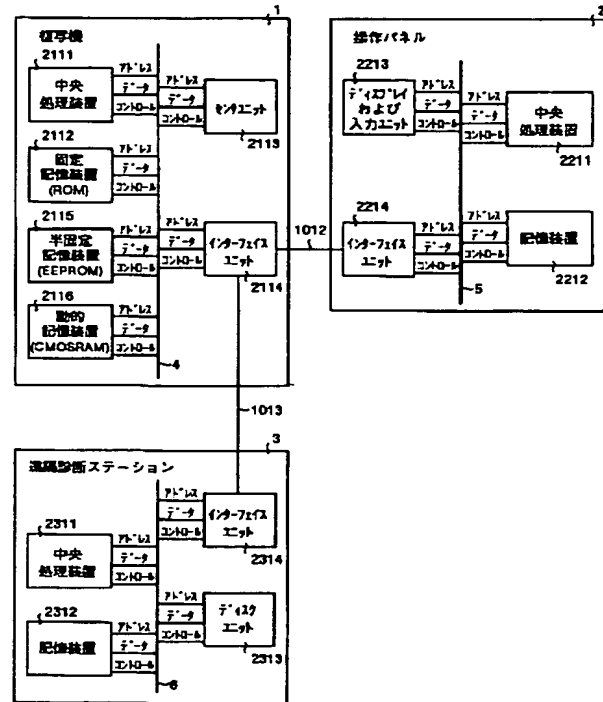
(c) 値



不定

00H 00H

【図 2】



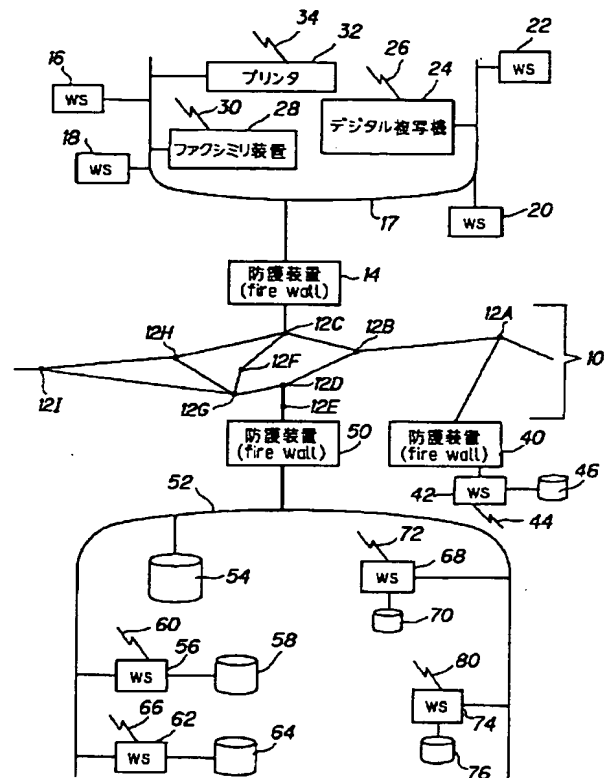
【図 4】

装置	パネル	データ	注釈
パワーオン	パワーオン		
1	→---	02, 81, 02	パネルとしての識別 装置はパワーオンリセット のため多忙
2	-----	02, 81, 01	装置自身の識別
3	→---	01, 81, 02	識別の確認
4	→---	02, 81, 02	最初の識別中断 再び試みる
5	→---	01, 81, 02	識別の確認 装置の確立
6	→---	03, 81, 04	特定のコピー数
7	→---	01, 81, 03	コピー数の確認
8	→---	04, 80	スタート
9	→---	01, 81, 04	スタートの確認
10	→---	61, 80	記録紙ジャム
11	→---	01, 81, 61	記録紙ジャムの確認

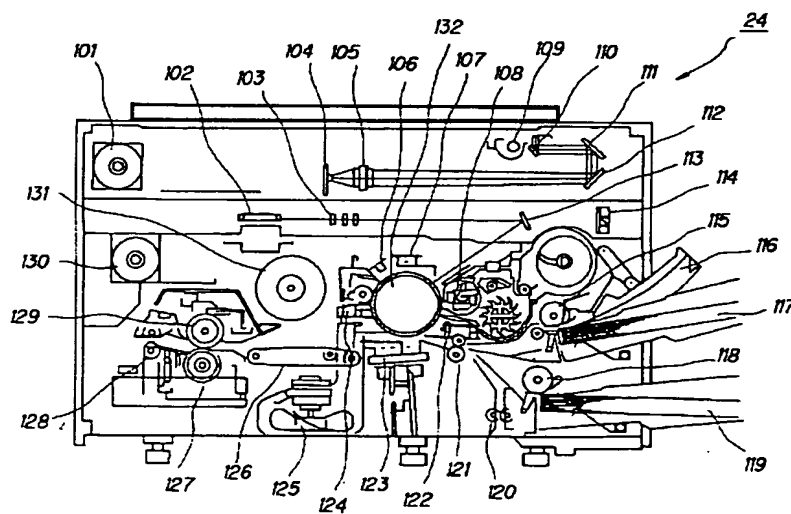
【図 5】

装置	参照ステーション	データ	注釈
1	-----	02, 81, 03	参照の識別
システム			
2	-----	01, 81, 02	識別の識別
3	-----	06, 81, 01	識別の問合せ
4	-----	41, 86, 01, 81, 06, 07, 81, 01	複合識別 問合せと複合の識別を識別=1
5	-----	06, 81, 02	モデルの問合せ
6	-----	41, 86, 01, 81, 06, 07, 81, 02	複合識別 問合せと複合の識別を識別=2
7	-----	09, 84, 00, 01, 00, 02	パラメータ(1,2)複合
8	-----	21, 81, 09	コマンド識別されず
9	-----	08, 84, 00, 00, 01, C1	アドレスの報告 (C1 C1)
内蔵			
10	-----	01, 81, 08	識別
11	-----	07, 87, 00, 00, 01, C1, 30, FF	報告 01C1=FF
12	-----	01, 81, 07	識別

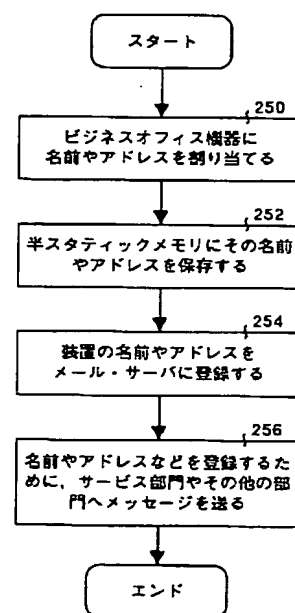
【図 6】



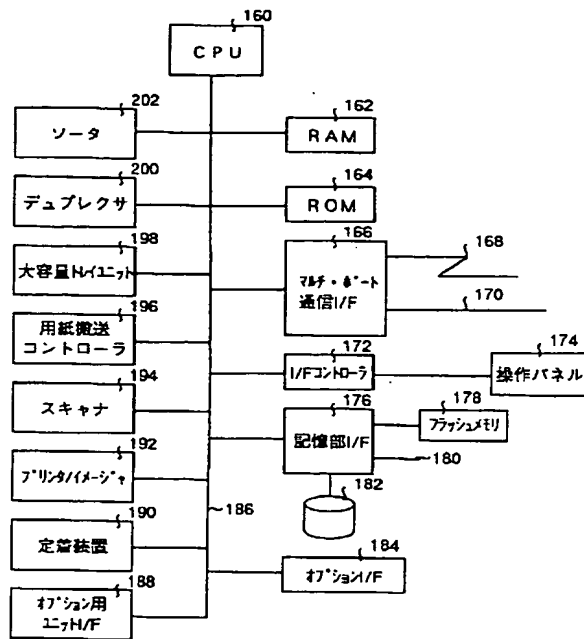
【図 7】



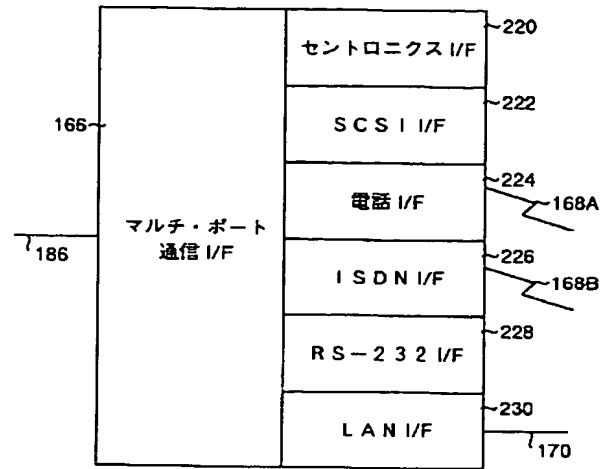
【図 10】



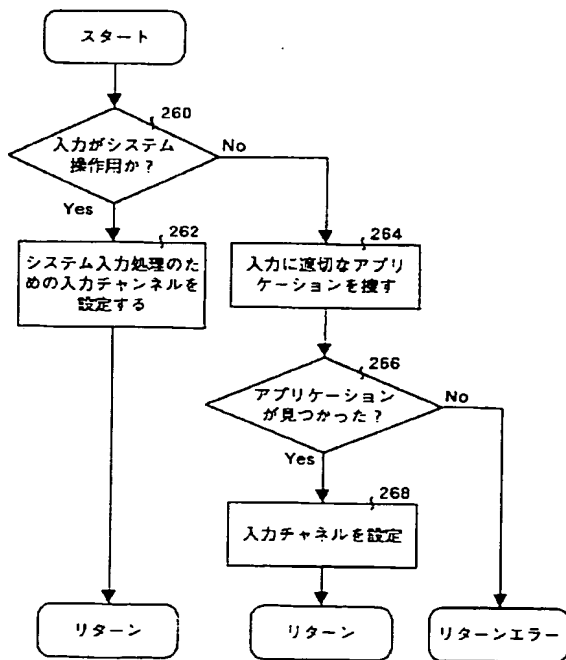
【図 8】



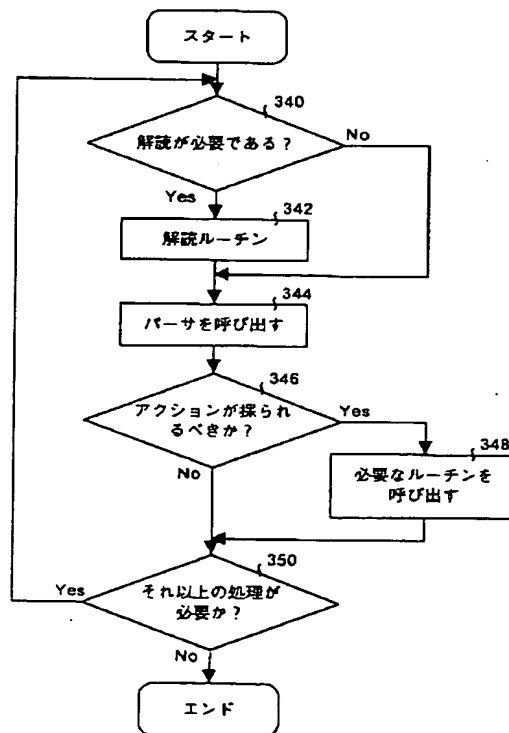
【図 9】



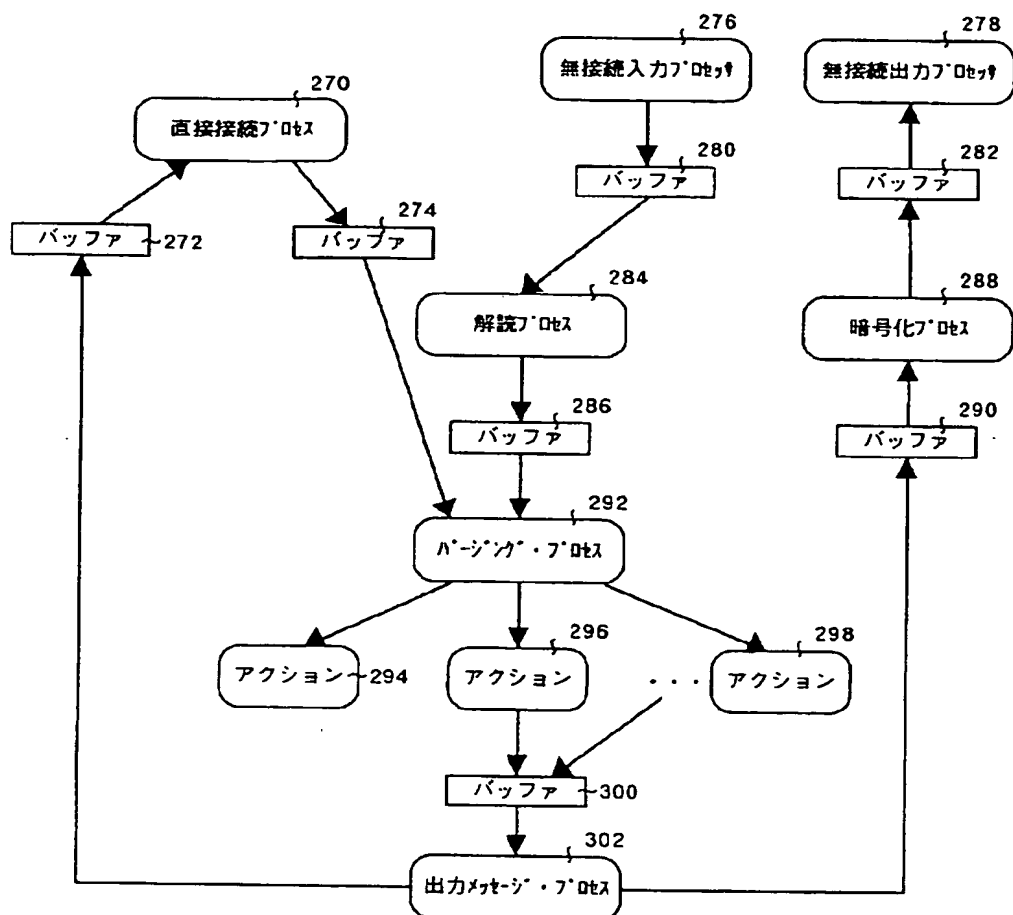
【図 11】



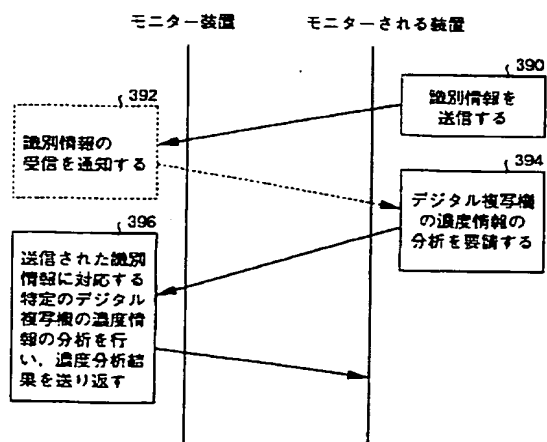
【図 13】



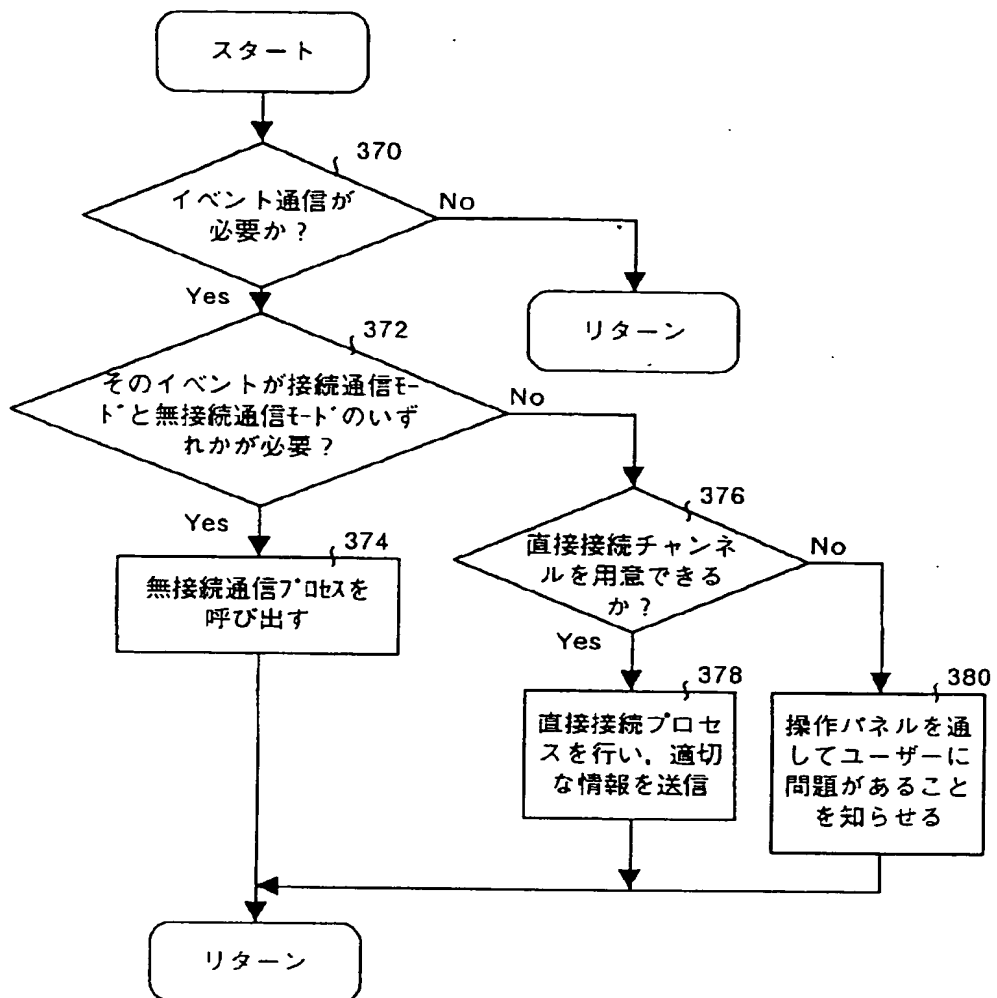
【図12】



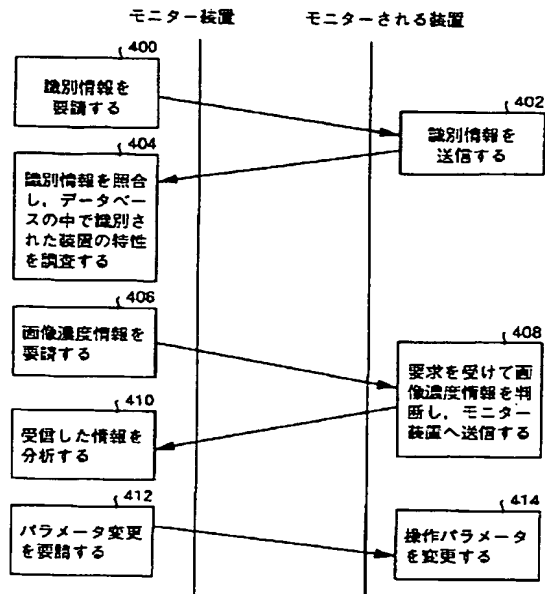
【図15】



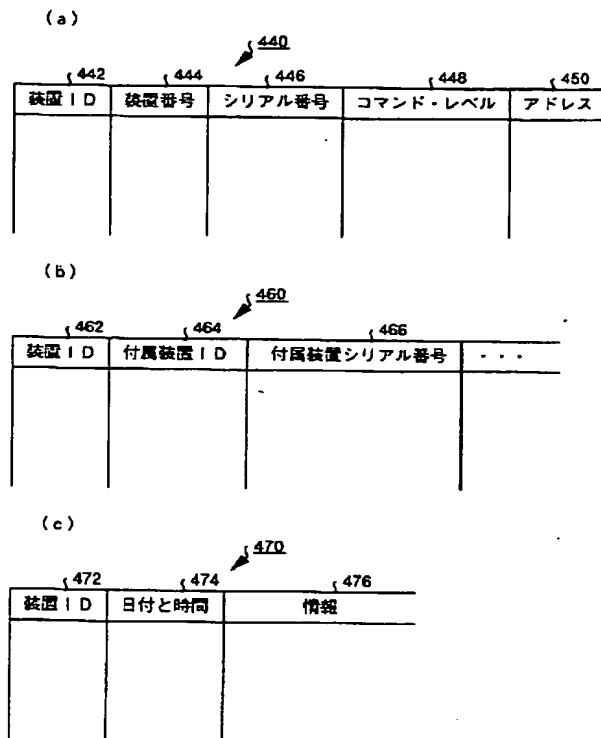
【図14】



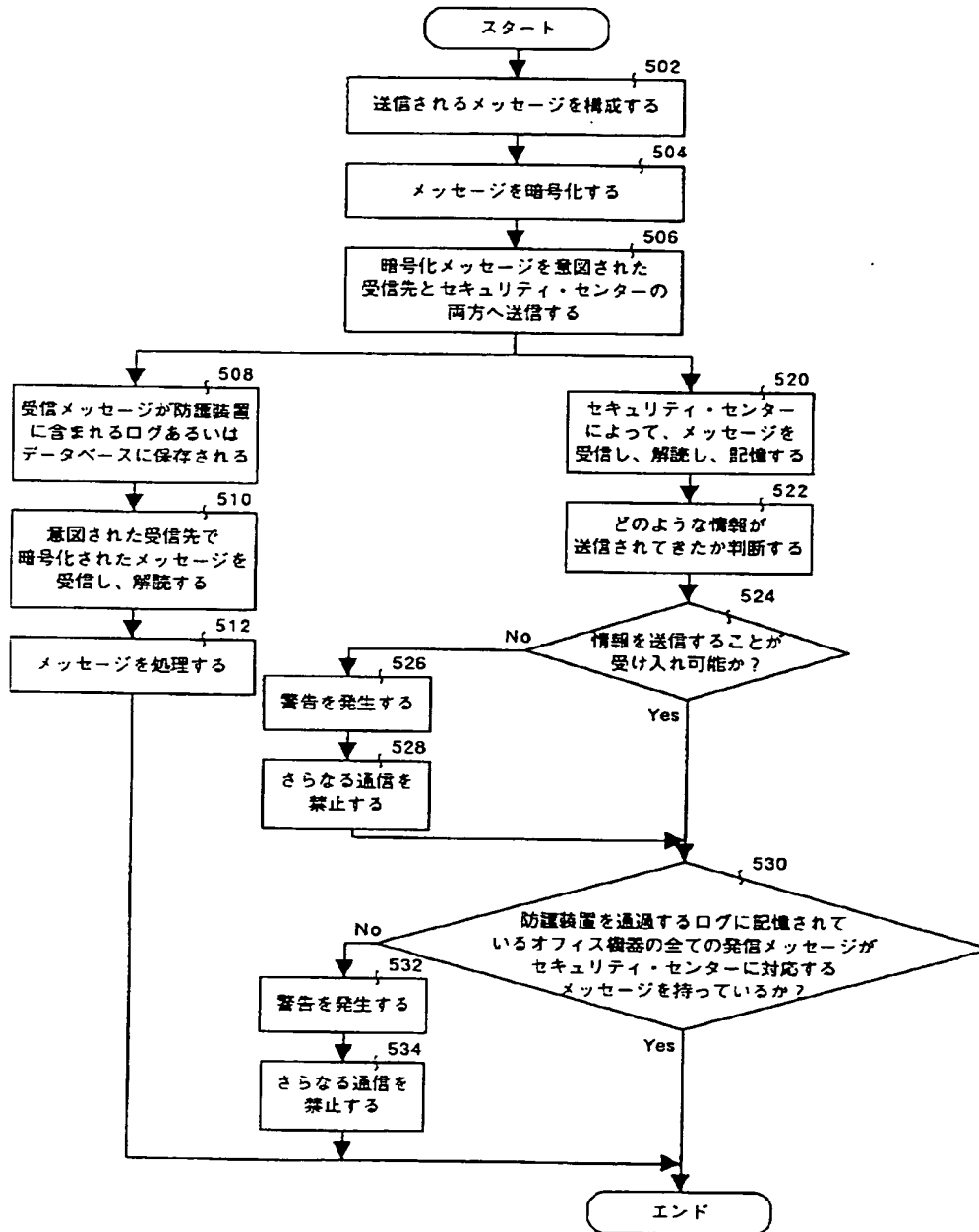
【図 16】



【図 17】



【図 18】



【図19】

